Stephanie Vergil

Lab 6: Introduction to Zeek Scripting

2.1 Starting a new instance of Zeek.

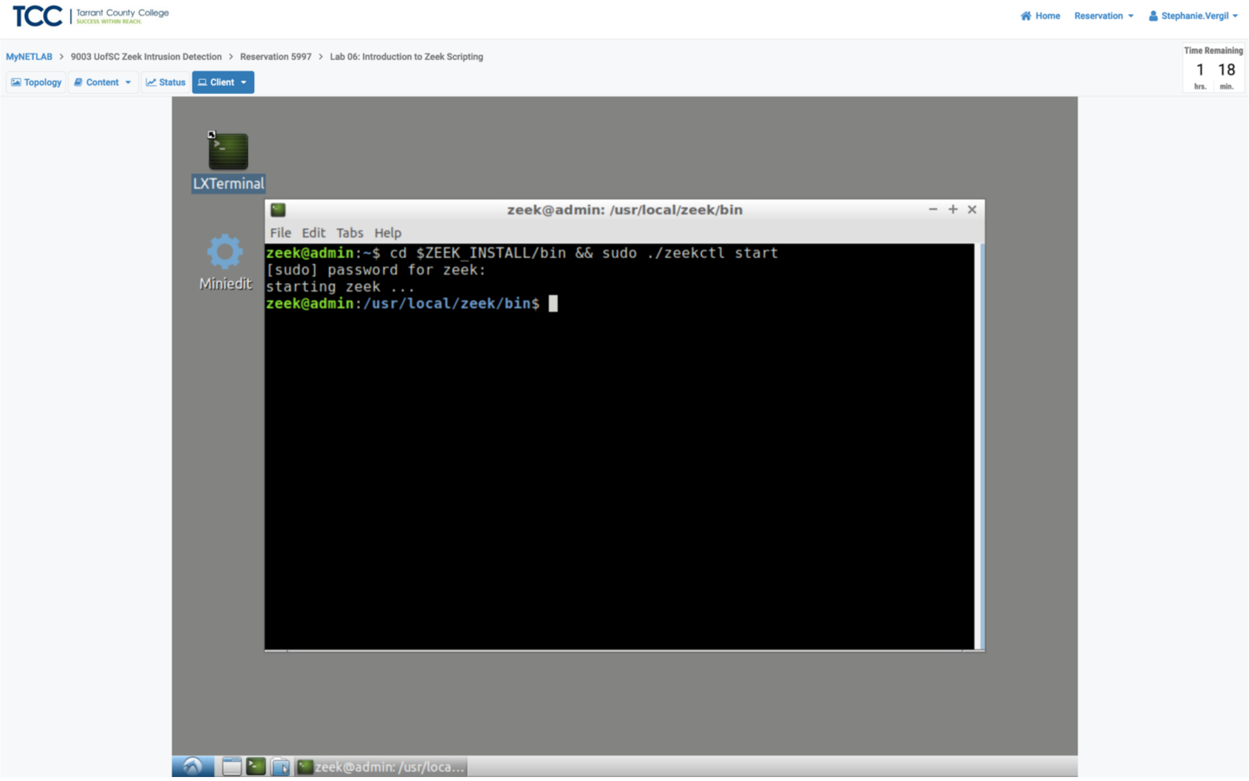
Step 1. Click on client button to launch the client machine.

Step 2. Located at the desktop from the client's machine launch LXTerminal by double clicking.

Step 3. To begin running Zeek, execute the following command in your terminal:

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

This command navigates to Zeek's default installation directory and utilizes the Zeekctl tool to initiate a new instance.



```
zeek@admin:~$ cd $ZEEK_INSTALL/bin && sudo ./zeekctl start
[sudo] password for zeek:
starting zeek ...
zeek@admin:/usr/local/zeek/bin$
```

2.2 Executing a UDP Zeek script

Step 1. To navigate to the Lab-Scripts directory enter the following command:

cd ~/Zeek-Labs/Lab-Scripts/

In this directory, all scripts can be accessed, modified, and viewed.

Step 2. Enter the following command to display the content of the lab6_sec2-2.zeek:

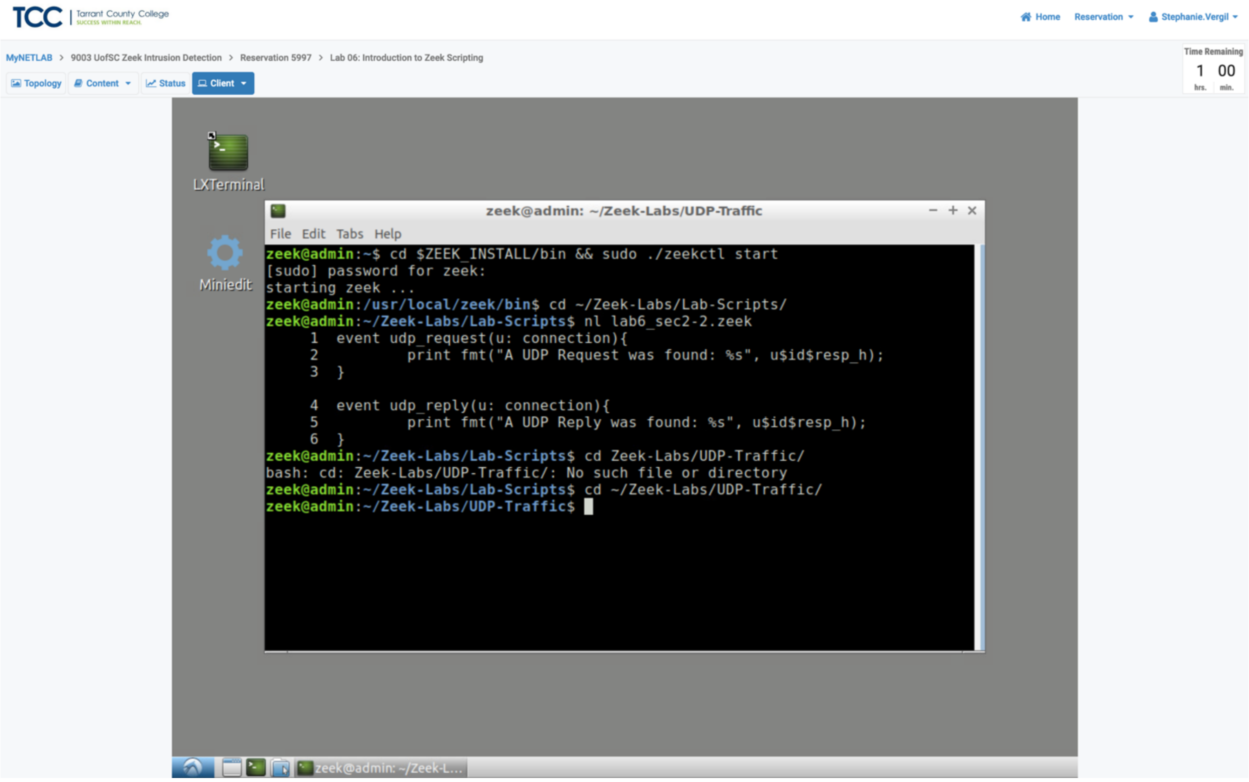
nl lab6_sec2-2.zeek

The nl command shows the line numbers in the file.

1. Triggers on processing UDP Request packets, storing related header details in 'u'.
2. Prints a string with '%s' for variable position, using 'u$id$resp_h' to get destination IP.
3. Ends 'udp_request' event.
4. Activates on processing UDP Reply packets, storing header info in 'u'.
5. Prints string, fetching destination IP with 'u$id$resp_h'.
6. Ends 'udp_reply' event.

Step 3. To navigate to the UDP-Traffic workspace directory enter the following command:

cd Zeek-Labs/UDP-Traffic/

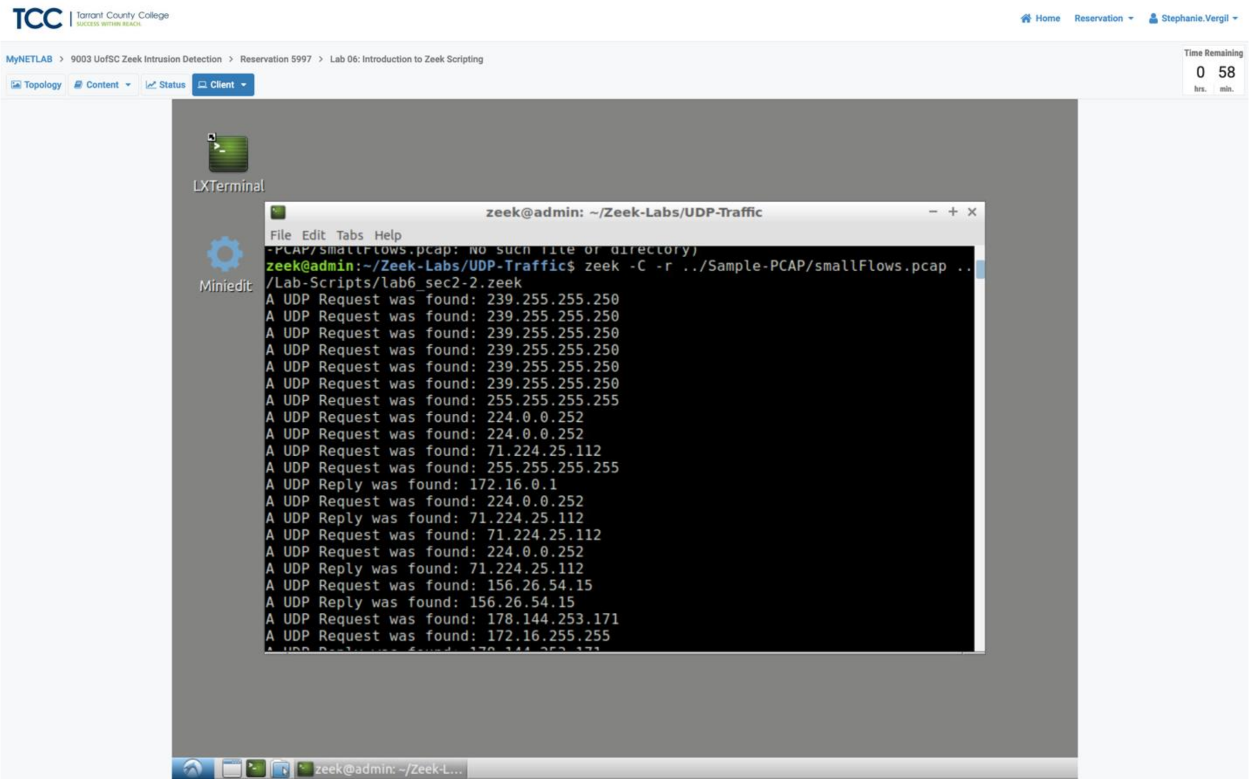


zeek@admin: ~/Zeek-Labs/UDP-Traffic

```
zeek@admin:~$ cd $ZEEK_INSTALL/bin && sudo ./zeekctl start
[sudo] password for zeek:
starting zeek ...
zeek@admin:/usr/local/zeek/bin$ cd ~/Zeek-Labs/Lab-Scripts/
zeek@admin:~/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@admin:~/Zeek-Labs/Lab-Scripts$ cd Zeek-Labs/UDP-Traffic/
bash: cd: Zeek-Labs/UDP-Traffic/: No such file or directory
zeek@admin:~/Zeek-Labs/Lab-Scripts$ cd ~/Zeek-Labs/UDP-Traffic/
zeek@admin:~/Zeek-Labs/UDP-Traffic$ 
```

Step 4. Enter the following command to process a packet capture file using the Zeek script. You may also use tab key to autocomplete the longer paths.

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


TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Topology
Content
Status
Client
Time Remaining
0 hrs. 58 min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/UDP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
-PCAP/smallFlows.pcap: No such file or directory)
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/smallFlows.pcap ..
/Lab-Scripts/lab6_sec2-2.zeek
A UDP Request was found: 239.255.255.250
A UDP Request was found: 239.255.255.250
A UDP Request was found: 239.255.255.250
A UDP Request was found: 239.255.255.250
A UDP Request was found: 239.255.255.250
A UDP Request was found: 239.255.255.250
A UDP Request was found: 255.255.255.255
A UDP Request was found: 224.0.0.252
A UDP Request was found: 224.0.0.252
A UDP Request was found: 71.224.25.112
A UDP Request was found: 255.255.255.255
A UDP Reply was found: 172.16.0.1
A UDP Request was found: 224.0.0.252
A UDP Reply was found: 71.224.25.112
A UDP Request was found: 71.224.25.112
A UDP Request was found: 224.0.0.252
A UDP Reply was found: 71.224.25.112
A UDP Request was found: 156.26.54.15
A UDP Reply was found: 156.26.54.15
A UDP Request was found: 178.144.253.171
A UDP Request was found: 172.16.255.255
A UDP Reply was found: 178.144.253.171
```

When we look at the captured data, the script shows stuff on the screen because we didn't set up anything special. When it sees certain events related to UDP packets, it tells us about them.

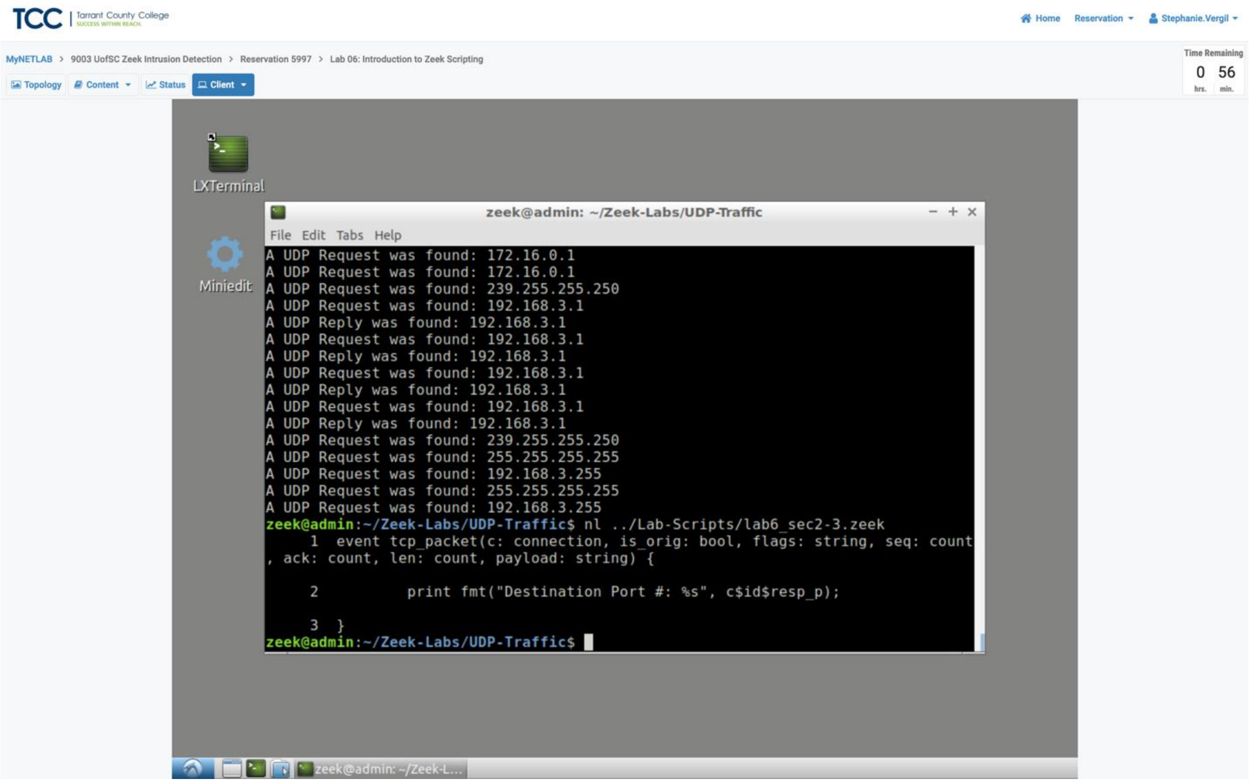
2.3 Executing a TCP Zeek script

Step 1. Enter the following command to display the content of the lab6_sec2-3.zeek :

nl ../Lab-Scripts/lab6_sec2-3.zeek

When a packet with a TCP header is handled, the script gathers information about the packet and stores it using the 'u' variable. Other TCP-related details are also collected in the same way.

It displays a specific message. '%s' serves as a placeholder for variable information within the string. Here, 'u$id$resp_h' is used to retrieve the destination address.

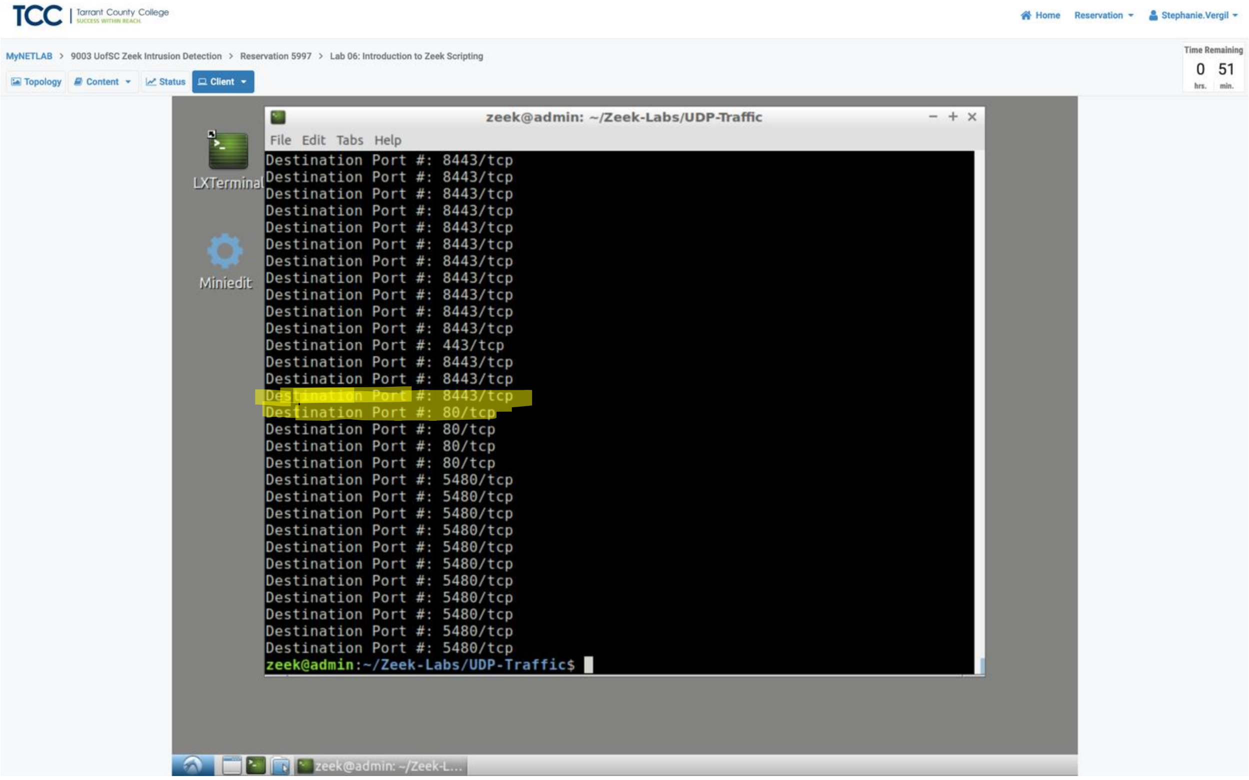

TCC | Tarrant County College
SUCCESS WITHIN REACH
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Topology
Content
Status
Client
Time Remaining
0 hrs. 56 min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/UDP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
A UDP Request was found: 172.16.0.1
A UDP Request was found: 172.16.0.1
A UDP Request was found: 239.255.255.250
A UDP Request was found: 192.168.3.1
A UDP Reply was found: 192.168.3.1
A UDP Request was found: 192.168.3.1
A UDP Reply was found: 192.168.3.1
A UDP Request was found: 192.168.3.1
A UDP Reply was found: 192.168.3.1
A UDP Request was found: 192.168.3.1
A UDP Reply was found: 192.168.3.1
A UDP Request was found: 239.255.255.250
A UDP Request was found: 255.255.255.255
A UDP Request was found: 192.168.3.255
A UDP Request was found: 255.255.255.255
A UDP Request was found: 192.168.3.255
zeek@admin:~/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@admin:~/Zeek-Labs/UDP-Traffic$ 
```

Step 2. Enter the following command to process a packet capture file using the Zeek script:

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

This will produce the following output on the screenshot bellow.


TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Topology
Content
Status
Client
Time Remaining
0 hrs.
51 min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/UDP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
zeek@admin:~/Zeek-Labs/UDP-Traffic$
```

When the tcp_packet event occurs, it shows the packet details. An example of Port 8443 and Port 80 traffic is highlighted. These examples demonstrate Zeek's ability to monitor particular types of traffic. For example, a script could be created to gather all Port 80 traffic each day and save it to a log file.

3 Modifying Zeek log streams

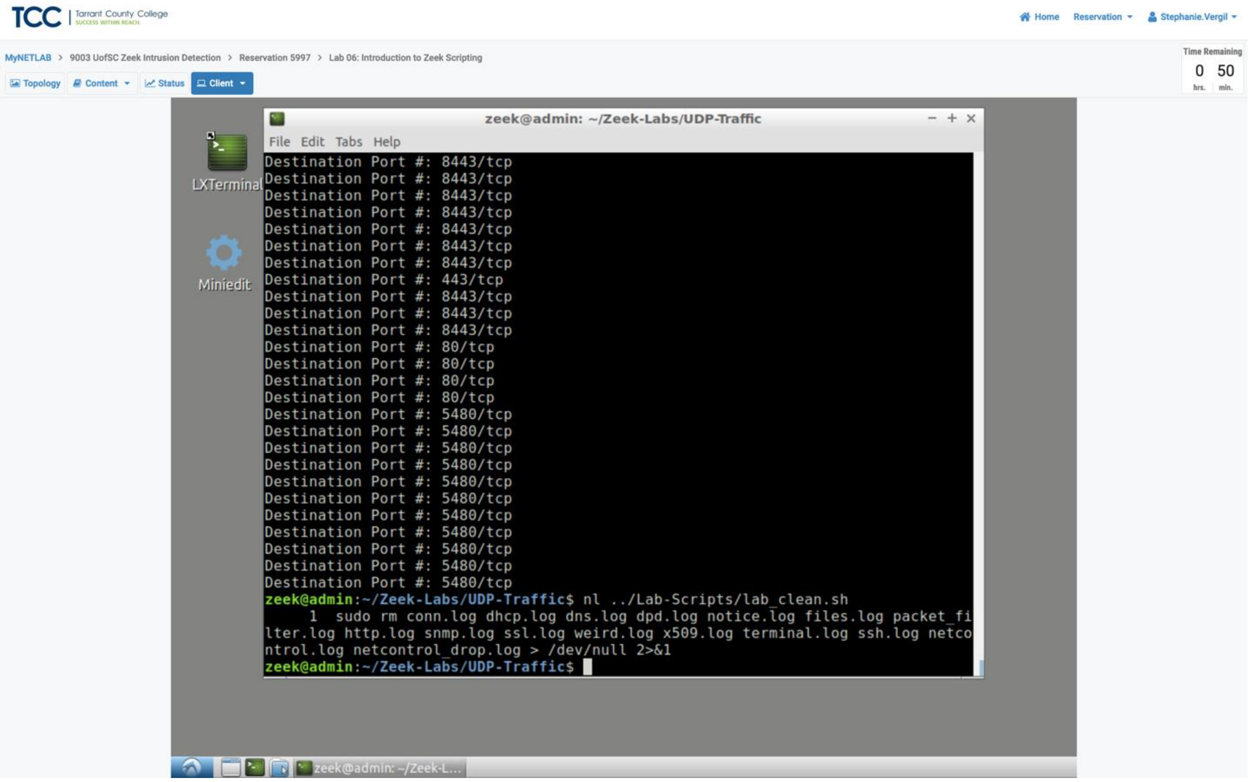
Zeek log streams control where an event's output goes and how it looks. You can add new streams, change default ones, or delete them. Before we move forward, you'll need to clean up the lab workspace directory.

Step 1. Enter the following command to display the contents of the of the lab_clean.sh shell script using nl command.

nl ../Lab-Scripts/lab_clean.sh

The shell script removes a set of files that Zeek typically generates during processing with its default log streams. Running this script will delete any log files previously generated in the directory. Output messages from executing this script won't appear in the Terminal;

instead, the code "> /dev/null 2>&1" directs errors and notices to a null folder, effectively suppressing them.

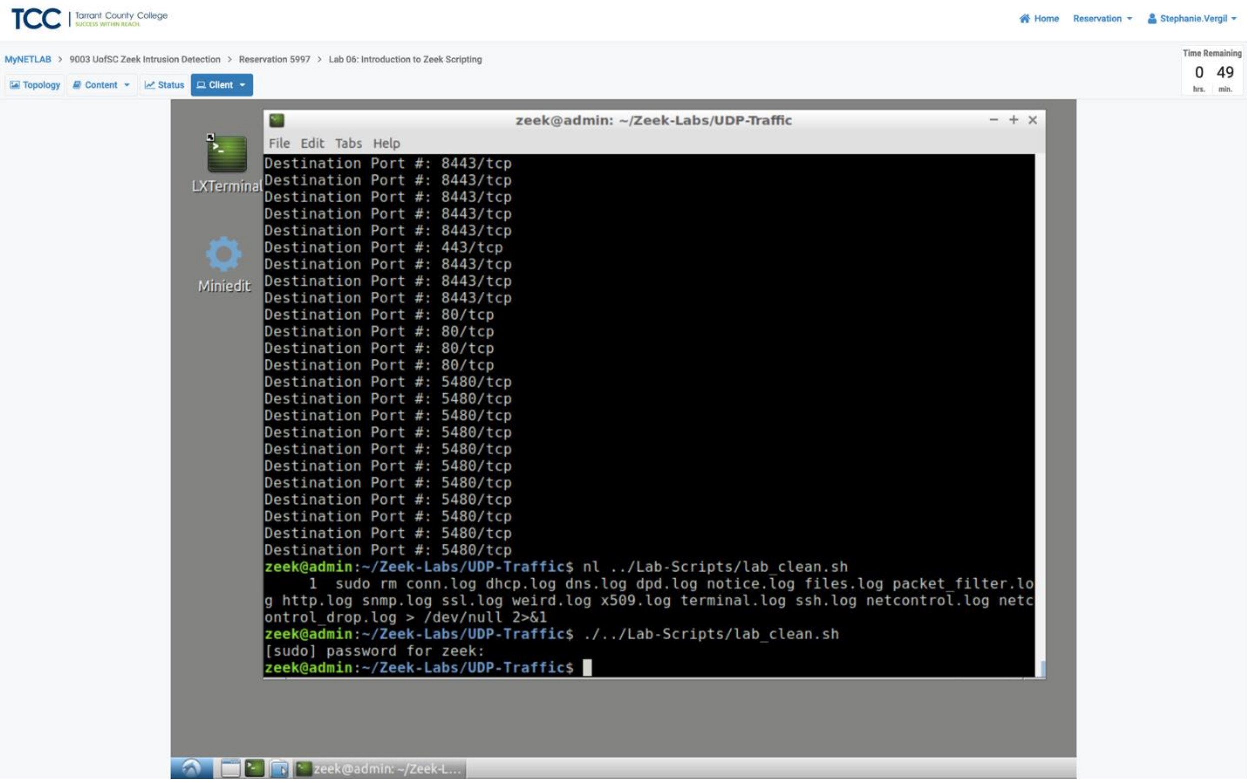

TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Time Remaining
0 hrs. 50 min.
Topology
Content
Status
Client
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/UDP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
zeek@admin:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab_clean.sh
     1	sudo rm conn.log dhcp.log dns.log dpd.log notice.log files.log packet_fi
lter.log http.log snmp.log ssl.log weird.log x509.log terminal.log ssh.log netco
ntrol.log netcontrol_drop.log > /dev/null 2>&1
zeek@admin:~/Zeek-Labs/UDP-Traffic$ 
```

Step 2. Enter the following command to execute the lab_clean.sh shell script:

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

Enter password when prompt to continue.


TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Time Remaining
0 hrs. 49 min.
Topology
Content
Status
Client
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/UDP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

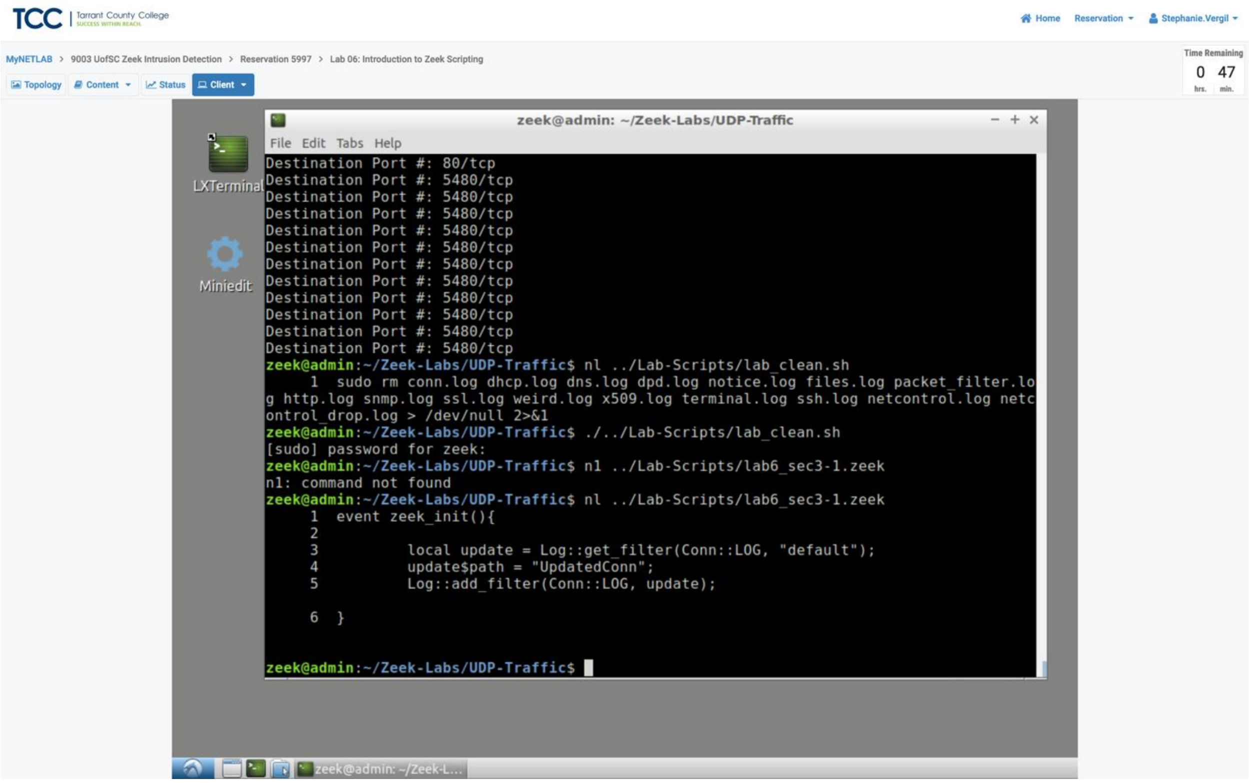
```
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 8443/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
zeek@admin:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab_clean.sh
     1  sudo rm conn.log dhcp.log dns.log dpd.log notice.log files.log packet_filter.lo
g http.log snmp.log ssl.log weird.log x509.log terminal.log ssh.log netcontrol.log netc
ontrol_drop.log > /dev/null 2>&1
zeek@admin:~/Zeek-Labs/UDP-Traffic$ ./../Lab-Scripts/lab_clean.sh
[sudo] password for zeek:
zeek@admin:~/Zeek-Labs/UDP-Traffic$ 
```

3.1 Renaming the conn.log stream

In this example, we'll change the name of the conn.log file to UpdatedConn.log. Renaming log streams can aid in organizing files, particularly if a log file has been altered from its original purpose.

Step 1. Enter the following command to display the contents of the lab6_sec3-1.zeek :

nl ../Lab-Scripts/lab6_sec3-1.zeek


TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Topology
Content
Status
Client
Time Remaining
0 hrs. 47 min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/UDP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
Destination Port #: 80/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
zeek@admin:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab_clean.sh
     1  sudo rm conn.log dhcp.log dns.log dpd.log notice.log files.log packet_filter.lo
g http.log snmp.log ssl.log weird.log x509.log terminal.log ssh.log netcontrol.log netc
ontrol_drop.log > /dev/null 2>&1
zeek@admin:~/Zeek-Labs/UDP-Traffic$ ./../Lab-Scripts/lab_clean.sh
[sudo] password for zeek:
zeek@admin:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab6_sec3-1.zeek
nl: command not found
zeek@admin:~/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  }


zeek@admin:~/Zeek-Labs/UDP-Traffic$ 
```

The script is explained as follows. Each number represents the respective line number:

1. Activates when Zeek is initialized.
3. Defines a local variable named "update" with the default Conn::LOG filter.
4. Specifies the path of the "update" variable as UpdatedConn.log.
5. Adds the new filter to the active log streams.
6. Concludes the zeek_init event.

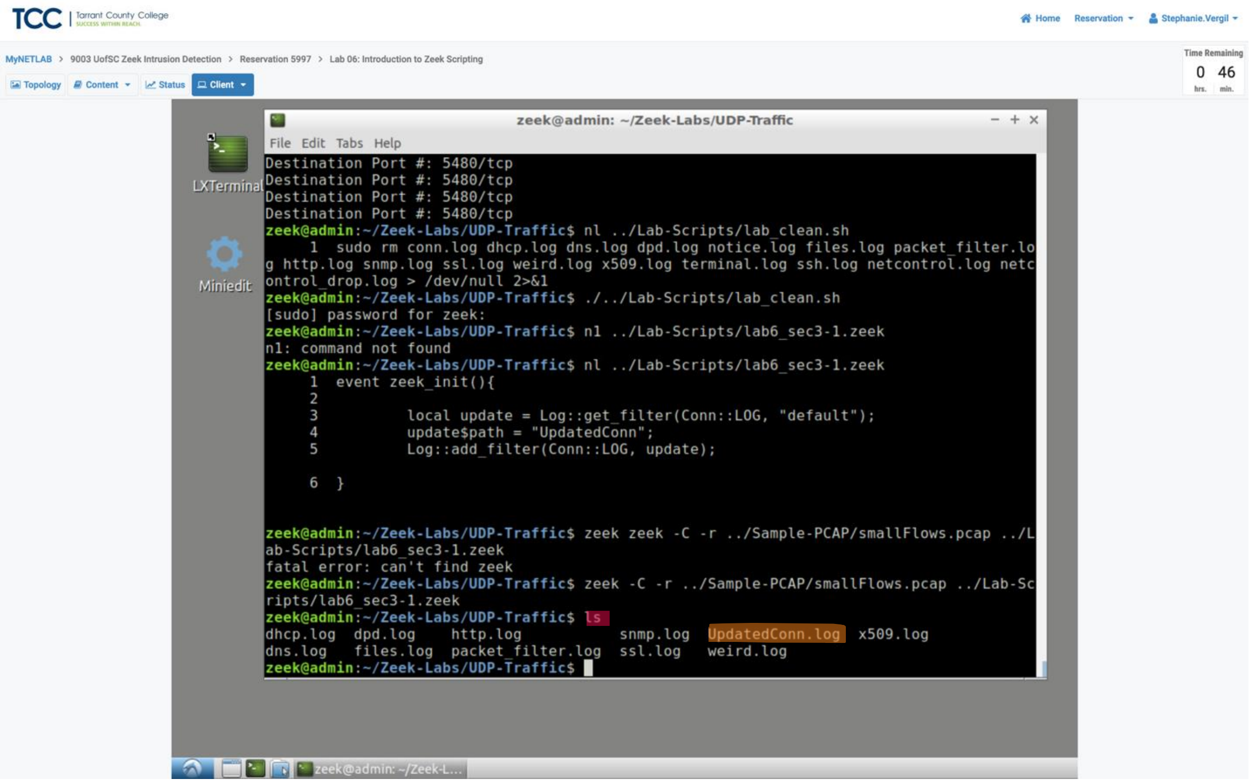
Step 2. Enter the following command to process a packet capture file using the Zeek script:

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

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

ls

Note the UpdatedConn.log, highlighted by the orange box. Since we did not change any formatting, it is an exact replica of the original conn.log file.


TCC | Tarrant County College
SUCCESS WITHIN REACH
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Topology
Content
Status
Client
Time Remaining
0 hrs. 46 min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/UDP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
Destination Port #: 5480/tcp
zeek@admin:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab_clean.sh
     1  sudo rm conn.log dhcp.log dns.log dpd.log notice.log files.log packet_filter.lo
g http.log snmp.log ssl.log weird.log x509.log terminal.log ssh.log netcontrol.log netc
ontrol_drop.log > /dev/null 2>&1
zeek@admin:~/Zeek-Labs/UDP-Traffic$ ./../Lab-Scripts/lab_clean.sh
[sudo] password for zeek:
zeek@admin:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab6_sec3-1.zeek
nl: command not found
zeek@admin:~/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  }


zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek zeek -C -r ../Sample-PCAP/smallFlows.pcap ../L
ab-Scripts/lab6_sec3-1.zeek
fatal error: can't find zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/smallFlows.pcap ../Lab-Sc
ripts/lab6_sec3-1.zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ ls
dhcp.log  dpd.log    http.log           snmp.log  UpdatedConn.log  x509.log
dns.log   files.log  packet_filter.log  ssl.log   weird.log
zeek@admin:~/Zeek-Labs/UDP-Traffic$ 
```

3.2 Updating the conn.log stream.

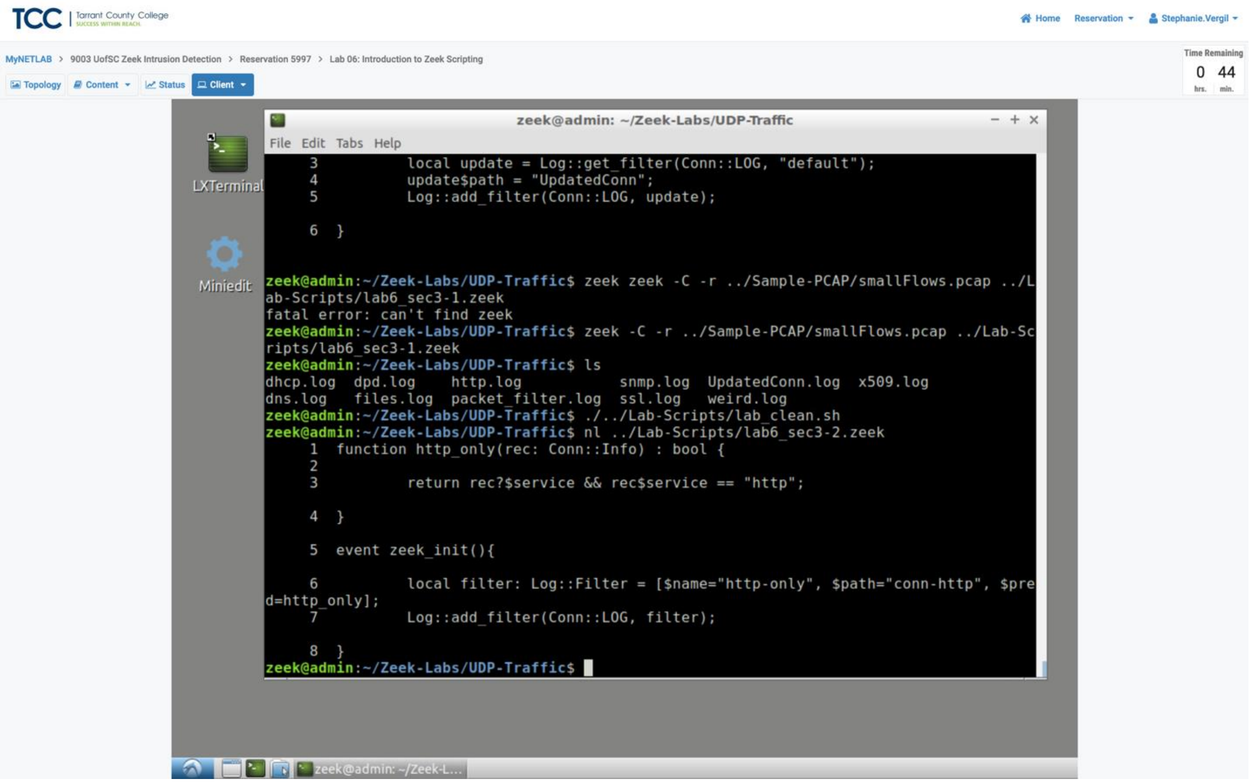
In this example, we're altering the conn.log file to produce an additional conn-http.log file. This adjustment divides the contents of conn.log between two log files, which proves helpful in organizing particular events—like segregating UDP traffic from TCP traffic, or separating reply messages from requests.

Step 1. Enter the following command to execute the included lab_clean.sh shell script:

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

Step 2. Enter the following command to display the content of of lab6_sec3-1.zeek Zeek script using the nl command:

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


TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Topology
Content
Status
Client
Time Remaining
0 hrs. 44 min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/UDP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
     3          local update = Log::get_filter(Conn::LOG, "default");
     4          update$path = "UpdatedConn";
     5          Log::add_filter(Conn::LOG, update);

     6  }


zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek zeek -C -r ../Sample-PCAP/smallFlows.pcap ../L
ab-Scripts/lab6_sec3-1.zeek
fatal error: can't find zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/smallFlows.pcap ../Lab-Sc
ripts/lab6_sec3-1.zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ ls
dhcp.log  dpd.log    http.log           snmp.log  UpdatedConn.log  x509.log
dns.log   files.log  packet_filter.log  ssl.log   weird.log
zeek@admin:~/Zeek-Labs/UDP-Traffic$ ./../Lab-Scripts/lab_clean.sh
zeek@admin:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab6_sec3-2.zeek
     1  function http_only(rec: Conn::Info) : bool {
     2
     3          return rec?$service && rec$service == "http";

     4  }

     5  event zeek_init(){

     6          local filter: Log::Filter = [$name="http-only", $path="conn-http", $pre
d=http_only];
     7          Log::add_filter(Conn::LOG, filter);

     8  }
zeek@admin:~/Zeek-Labs/UDP-Traffic$ 
```

The script is explained as follows. Each number represents the respective line number:

1. Boolean function that has the parameter rec, an instance of Conn::Info. 3. Returns True if the service stored in rec is the HTTP protocol.

4. End of the function.

5. Event zeek_init is activated when Zeek is first initialized.

6. Creates a local filter with http related naming and pathing.

7. Appends the new filter to the active log streams.

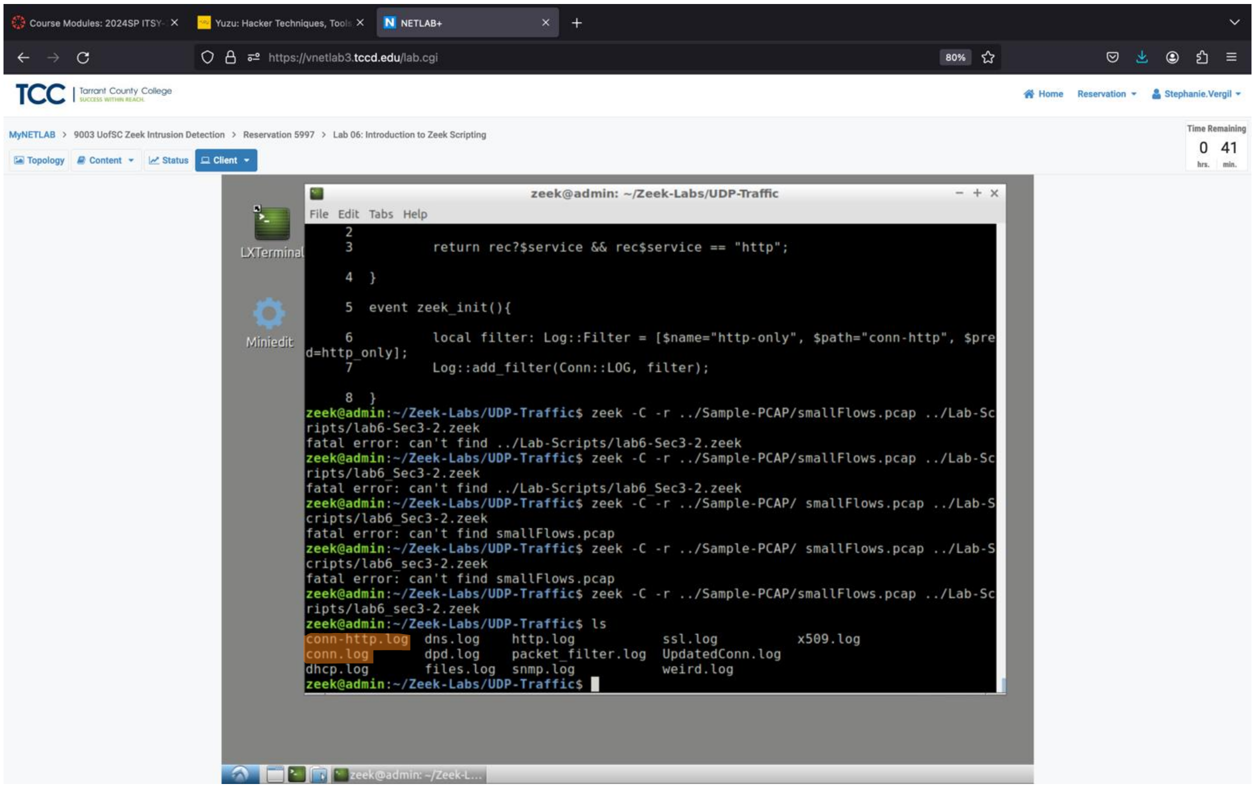
8. End of the zeek_init event.

Step 3. Enter the following command to process a packet capture file using the Zeek script:

zeek –C -r ../Sample-PCAP/ smallFlows.pcap ../Lab-Scripts/lab6_sec3-2.zeek

Step 4. Enter the following command to list the generated log files in the current directory:

ls


Course Modules: 2024SP ITSY
Yuzu: Hacker Techniques, Tools
NETLAB+
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC | Tarrant County College
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Time Remaining
0 hrs.
41 min.
Topology
Content
Status
Client
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/UDP-Traffic
File
Edit
Tabs
Help
zeek@admin: ~/Zeek-L...

```
     2
     3          return rec?$service && rec$service == "http";

     4  }

     5  event zeek_init(){

     6          local filter: Log::Filter = [$name="http-only", $path="conn-http", $pre
d=http_only];
     7          Log::add_filter(Conn::LOG, filter);

     8  }
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/smallFlows.pcap ../Lab-Sc
ripts/lab6-Sec3-2.zeek
fatal error: can't find ../Lab-Scripts/lab6-Sec3-2.zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/smallFlows.pcap ../Lab-Sc
ripts/lab6_Sec3-2.zeek
fatal error: can't find ../Lab-Scripts/lab6_Sec3-2.zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/ smallFlows.pcap ../Lab-S
cripts/lab6_Sec3-2.zeek
fatal error: can't find smallFlows.pcap
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/ smallFlows.pcap ../Lab-S
cripts/lab6_sec3-2.zeek
fatal error: can't find smallFlows.pcap
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/smallFlows.pcap ../Lab-Sc
ripts/lab6_sec3-2.zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ ls
conn-http.log  dns.log    http.log           ssl.log          x509.log
conn.log       dpd.log    packet_filter.log  UpdatedConn.log
dhcp.log       files.log  snmp.log           weird.log
zeek@admin:~/Zeek-Labs/UDP-Traffic$
```

Note: The conn-http.log file in the first column. This file will maintain the same formatting as the conn.log file but will exclusively contain HTTP traffic. These files are highlighted within the orange box in the following image.

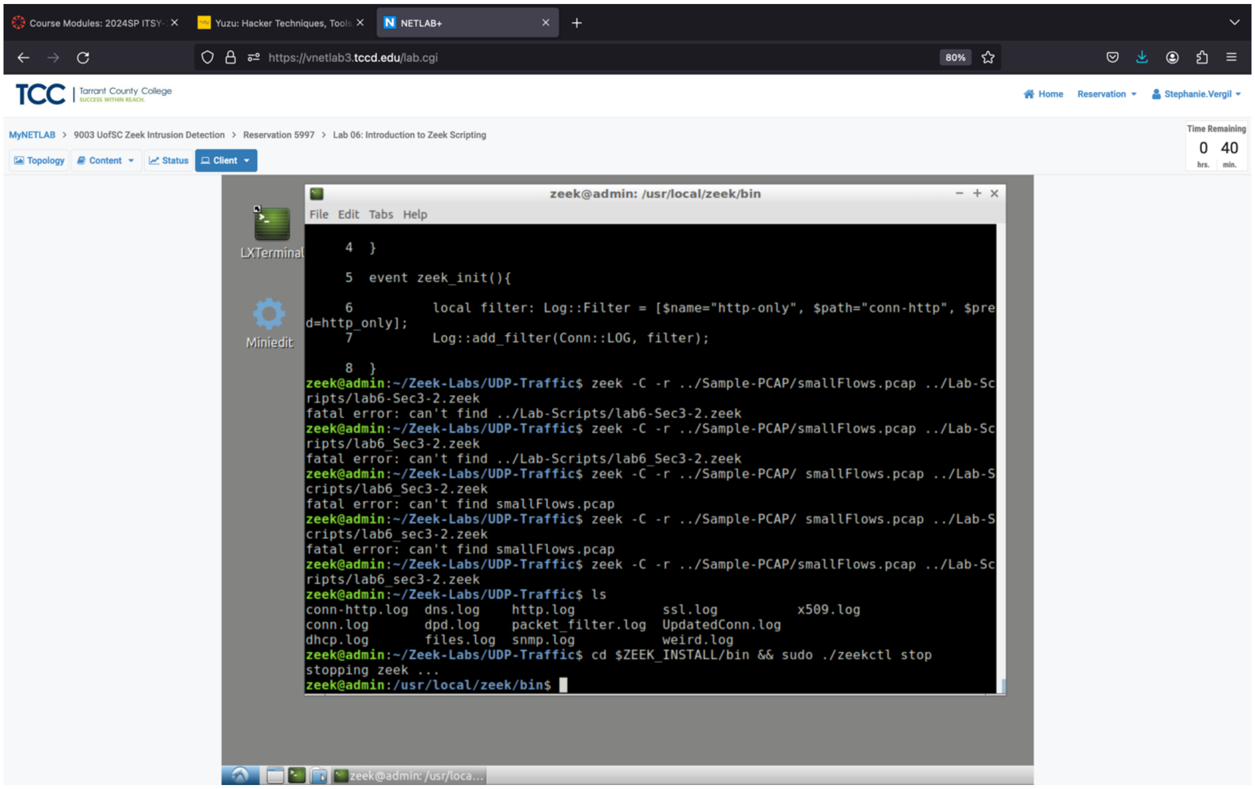
3.3 Closing the current instance of Zeek

Closing the current Zeek instance is essential once you've completed the lab. Leaving an active instance running and shutting down the computer can lead to Zeek shutting down improperly, potentially causing errors in future instances.

Step 1. To Stop Zeek enter the following command on the terminal:

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

Stephanie Vergil


Course Modules: 2024SP ITSY-
Yuzu: Hacker Techniques, Tools
NETLAB+
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC | Tarrant County College SUCCESS WITHIN REACH
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9003 UofSC Zeek Intrusion Detection > Reservation 5997 > Lab 06: Introduction to Zeek Scripting
Time Remaining
0 hrs. 40 min.
Topology
Content
Status
Client
LXTerminal
Miniedit
zeek@admin: /usr/local/zeek/bin
File
Edit
Tabs
Help
zeek@admin: /usr/loca...

```
     4  }

     5  event zeek_init(){

     6          local filter: Log::Filter = [$name="http-only", $path="conn-http", $pre
d=http_only];
     7          Log::add_filter(Conn::LOG, filter);

     8  }
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/smallFlows.pcap ../Lab-Sc
ripts/lab6-Sec3-2.zeek
fatal error: can't find ../Lab-Scripts/lab6-Sec3-2.zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/smallFlows.pcap ../Lab-Sc
ripts/lab6_Sec3-2.zeek
fatal error: can't find ../Lab-Scripts/lab6_Sec3-2.zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/ smallFlows.pcap ../Lab-S
cripts/lab6_Sec3-2.zeek
fatal error: can't find smallFlows.pcap
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/ smallFlows.pcap ../Lab-S
cripts/lab6_sec3-2.zeek
fatal error: can't find smallFlows.pcap
zeek@admin:~/Zeek-Labs/UDP-Traffic$ zeek -C -r ../Sample-PCAP/smallFlows.pcap ../Lab-Sc
ripts/lab6_sec3-2.zeek
zeek@admin:~/Zeek-Labs/UDP-Traffic$ ls
conn-http.log  dns.log    http.log           ssl.log          x509.log
conn.log       dpd.log    packet_filter.log  UpdatedConn.log
dhcp.log       files.log  snmp.log           weird.log
zeek@admin:~/Zeek-Labs/UDP-Traffic$ cd $ZEEK_INSTALL/bin && sudo ./zeekctl stop
stopping zeek ...
zeek@admin:/usr/local/zeek/bin$ 
```

Zeek scripts allow for customization of output log streams. Beyond simply renaming files, scripts enable the splitting of files to generate more protocol or event-specific log files. Zeek scripts serve as the foundation for establishing an organized workspace for storing and parsing generated log files.