**CYBR 440 - Incident Detection and Response  
Module 3 Lab – Collecting Network Evidence**

In this third lab, we will begin exploring some of the technical tools and data that are used in incident response. This lab specifically addresses the collection of network evidence. While we examine some common sources of network evidence, keep in mind that there are more sources of evidence than we have time to cover in this course. These labs take place in a fictional bank called Bellevue Bank and Trust. We will continue to utilize technology from this fictional bank for the remainder of the course.

**You will be required to submit the following graded items as part of this lab:**

* Answer all questions listed in **BOLD**
* Provide screenshots when asked

Accessing the Lab

This lab is hosted in the universities IS Lab and requires special instructions to access it. If you are not familiar with accessing the IS Lab, please see the document in this course that walks you through accessing the Cybersecurity Desktop. You can access the Cybersecurity Desktop through the Web or using VMWare’s Horizon client. You should use the native Horizon client when possible as it provides better performance. The web client can be accessed at2. Make sure you log into this interface with your Bellevue student ID and password.

After accessing workspace.bellevue.edu and selecting the IS Lab desktop, open a browser and navigate to <https://10.98.100.11>. The first time you access this site you will see a warning in the browser. Make sure to click advanced and then Proceed to 10.98.100.11 (Unsafe). You should see the following remote access page.

Graphical user interface, application, Word

Description automatically generated

After accessing Bellevue Bank and Trust’s Remote Management Portal, login in using the following information:

* Username: analyst# - Where # is the number provided to you by your instructor
* Password: An@lyst#!! - Where # is the number provided to you by your instructor

After logging in you should see the following page:

Graphical user interface, application

Description automatically generated

You should have three available connections, RDP Kali #, RDP Workstation#, and SSH Kali #. These are your three analyst tools you will use throughout this course.

You will be using the Windows 10 RDP Workstation# connection for this lab. You should open each new RDP or SSH connection in a new tab.

Part 1 - Examining Firewall and Netflow Logs

To complete this lab, you will be using and OPNSense firewall. This is a firewall that is freely available, but it also provides many of the same capabilities available on a commercial enterprise grade firewall. In this lab we will examine some of the information available directly on the firewall and some of the settings that allow the firewall logs to be exported to a SIEM called Graylog.

1. Right click the RDP Workstation# link. This will open up an RDP session to a Windows 10 desktop. If you encounter a login screen, your username and password to this Windows 10 desktop is the same as that used for the Remote Management Portal: analyst# and An@lyst#!!.

Logo

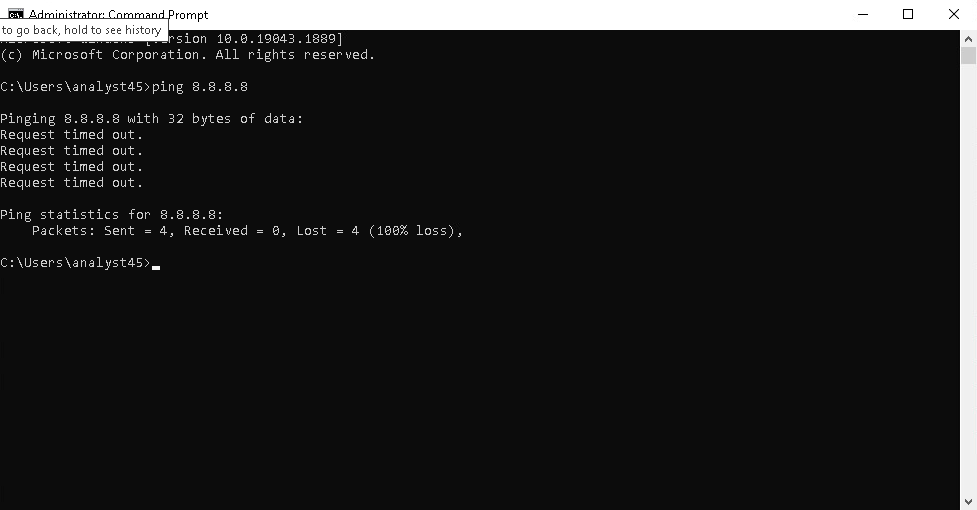
Description automatically generated

1. Open the shortcut on the desktop labeled OPNSense Management Interface or open a browser and go to <https://opnsense.bbtrust.com:8443>.
2. Log in using the username and password provided above: analyst# and An@lyst#!!. If you have successfully logged in, you should see the following screen:

Graphical user interface

Description automatically generated

1. Look at the left side of the screen. This menu bar represents all the actions you can within the firewall. Let’s start by looking at a live view of the firewall logs. Navigate to Firewall > Log Files > Live View. You will an interface that shows logs of firewall actions taken scrolling by. These actions are pass (allow) or block (deny) and are color coded accordingly.



1. Using the dropdown on the right side of the screen, select 250 and then click the refresh button. After you see some red lines scroll by, unselect the Auto Refresh and answer the following questions. If you do not see any blocks, type cmd.exe into the Type Here to Search textbox on the taskbar and open the command prompt. Then type ping 8.8.8.8. This will generate firewall blocks for ICMP messages.

**Pick one of the red lines and record the following data:**

**Interface: Lan**

**Source: 172.20.0.7:443**

**Destination: 172.28.37.254:19012**

**Protocol: Tcp**

**Label: Default deny/state violation rule**

These lines represent traffic that the firewall has been blocked and information associated with a block. Both the allowed and denied traffic are important when conducting an incident investigation.

**Paste a screenshot of the Firewall: Log Files: Live View Screen Below (Note: Use the Windows Snipping Tool or the shift+command+4 keys on Mac.Table

Description automatically generated**

1. Next we will see how we can configure the firewall to send the Firewall filter logs to our Graylog SIEM. Navigate to System > Settings > Logging. Notice that Log packets matched from the default block rules put in the ruleset and Log packets matched from the default pass ruleset are selected.
2. Now navigate to the System > Settings > Logging / targets page. Now click the pencil/edit button next to the only logging destination / hostname listed and answer the following questions.

Table

Description automatically generated

**What is the IP address of the Graylog SIEM Log Collector?**

**172.28.37.11**

**What is the TCP Port used to send logs to the Graylog SIEM Log Collector?**

**Port: 5514**

1. Now let’s look at another tools that are used to examine NetFlow data. Navigate to Reporting > Insights. This is a built-in tool that gives us graphs and statistics on the different flows on a network. Spend a few minutes looking at this page. And answer the following questions.

**What is the most used protocol identified by this firewall on the lan (graph in the second box on the left)?**

**http**

**Which IP address on the LAN has generated the most traffic over this time period?**

**172.28.37.109**

1. Next take a look at the Details tab and hit the refresh button on the right side of the screen. This page shows details about all the flows. The details can be filtered with the controls at the top of the page. Spend a few minutes looking over the details of this page.
2. Let’s look at another tool that looks and traffic and provides similar statistics to the Insights page. Navigate to Zenarmor-Sensei > Dashboard. Spend a few minutes looking through the dashboard.

**Which graphs, charts, maps, or statistics do you find the most helpful?**

I find the detailed graphs most helpful like the Unique local hosts overtime data.

Part 2 - Examining Firewall and NetFlow logs with a SIEM

1. Now we will look at one more NetFlow tool. Go to the address bar of your browser and enter <https://opnsense.bbtrust.com:3001>. This will bring you to another login and tools called NtopNG. Use your username of analyst# and password of An@lyst#!! where # is your analyst number. Look at the dashboard for a few minutes and navigate to each tab.
   1. The Talkers Tab shows a real time flow graph of current NetFlows
   2. The Hosts Tab shows a pie graph of the hosts with the most traffic.
   3. The Ports Tab shows pie graphs of the top used ports by number
   4. The Applications Tab shows a pie graph of the most used network applications
2. Navigate to Flows on the left side of the web page. This page shows details for recent TCP and UDP flow. Spend some time looking at each of the columns in the table. Pay special attention to the Client, Server, Duration, Breakdown and Actual Throughput. The Breakdown columns shows the different between data sent to the server vs data sent from the server. Spend a few minutes watching this table update.
3. Now let’s take our first look at an enterprise SIEM. We will use this tool to search NetFlow and firewall rule filters. Go to your browser address bar and navigate to either <https://graylog1.bbtrust.com:9000> or <https://graylog2.bbtrust.com:9000>. Log in using your username of analyst# and password of An@lyst#!!.
4. If you are not already on the Search page, click Search at the top of the page. From this page we will see the raw logs exported from the firewall. These logs include NetFlow records and firewall filter logs. Do the following:
   1. Type *filterlog* into the search box and hit search to see only the firewall filter logs. Spend a few minutes looking through the filter logs.
   2. Type *NetFlowV9* into the search box and press search to see only the NetFlow records.
   3. Open the first log by clicking on it. Here you can see the individual components of the log. Graylog Inputs/Collectors, when properly configured will take the individual components of the logs and separate them so that we use those components to search and filter on. We can even create graphs and charts.
      1. Click the + (Create) on the left side of the screen.
      2. Click Aggregation then click the right side of the screen where you want to place it. Make sure the Search still says NetFlowV9.
      3. Click edit in the new Untitled Aggregation.
      4. Click the + to the right of Group By.
      5. Select the following options
         1. Direction: Row
         2. Field: nf\_src\_address
         3. Limit: 15
      6. Select the + next to Metrics
         1. Function: Sum
         2. Field: nf\_bytes
         3. Name: Total Bytes
      7. Select the + next to Sort
         1. Field: Total Bytes
         2. Direction: Descending
      8. Click Update Preview (You may have to wait a few seconds)
      9. Let’s make this a bit prettier and change the Visualization to a Pie Chart.
         1. Visualization: Pie Chart
      10. Click Update Preview
      11. Click Apply Changes

**Take a screen shot of your pretty pie chart and paste it below.**

**A picture containing text, monitor, screenshot, computer

Description automatically generated**

Part 3 - Examining raw network traffic captures

1. Let’s look at the final two tools. Arkime (previously known as Moloch) and Wireshark. Arkime is a full-packet capture and analysis system. It passively monitors packets on a network and allows you search, sort, visualize, and download raw packet data. Go to your address bar and type <https://arkime.bbtrust.com>. Login using the username analyst# and password An@lyst#!!.
2. The Sessions page shows a timeseries chart. This represents that sessions/packets/bytes/data bytes over time. Beneath that is a list of session and associated packet captures. Pick a session and click on the green +.
3. Spend a few minutes looking at the information for the session. The top has the option to download a PCAP of the session, the source raw packets, destination raw packets, add tags (great for investigation) etc. It will also have detailed information on the encryption, application, transport and network protocols used in the session. The sent and received packets will be displayed in ASCII in blue in red at the bottom of the session (first 200 packets by default).
4. Scroll back to the top of session and click Download PCAP. Click on the downloaded file to open it in Wireshark. Wireshark will show many more details about this session and has many more tools. Spend a few minutes looking at the information available in Wireshark and then close Wireshark. We will be working exclusively with Wireshark for the Module 4 lab.
5. Click on the Connections Tab and then change the time period to Last year. This screen shows a connection chart for the different sessions Arkime has observed. Spend a few minutes examining other functions of Arkime and then complete the final question below.

**Take a screen shot of the Arkime connection chart and paste it below.A picture containing graphical user interface

Description automatically generated**