**CYBR 440 - Incident Detection and Response  
Module 4 Lab – Analyzing Network Evidence**

In this fourth lab, we will exclusively be using Wireshark to look for malicious traffic in raw packet captures. While this is something that we can do at multiple levels (raw packet captures, NetFlow records, firewall logs, etc.) understanding how to do this at the lowest level will you give you the fundamental knowledge to do it at any level. It will also allow you search for malicious traffic if you have only the most basic tools.

**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 - Malicious Scanning

The source PCAPs for these exercises can be found at https://www.malware-traffic-analysis.net/ . This is a blog site that shares malicious PCAPs and gives you the opportunity to improve your Wireshark skills. If you want some additional practice using Wireshark for examining malicious traffic, try reviewing these tutorials: <https://www.malware-traffic-analysis.net/tutorials/index.html>.

1. Start by opening the CYBR 440 - Shortcut folder on the Desktop then then navigate to Malicious Pcaps. Then open the 2019-12-25-traffic-analysis-exercise-alerts.jpg. This is a screen shot of an intrusion detection system and it shows a number of alerts for web connections between 139.199.184.166 and 10.12.25.101. Take a few minutes and read through the alerts listed under the Event Message columns. Take note of the two IP addresses.
2. Next, close the .jpg file and open the 2019-12-25-traffic-analysis-exercise-alerts.txt file. This text file is the log file associated with the GUI alerts seen in the .jpg file. Take a few minutes to look through the file. Notice that 10.12.25.101 and 139.199.184.166.
3. Close the text file and open the 2019-12-15-traffic-analysis-exercise.pcap file. Doubling click the file should open Wireshark and load the pcap file.
4. Let’s start by cleaning up our columns and making it more suitable to analyzing malicious traffic. Further instruction on how to do this can be found here: <https://unit42.paloaltonetworks.com/unit42-customizing-wireshark-changing-column-display/>. We will be doing the following.
   1. Removing the No., and Length columns.
   2. Adding the TCP source port and destination port columns
   3. Changing the time to UTC
   4. Add a custom HTTP host column
5. Right click the column headers for the packet list pane and unselect No. and Length
6. Right click the column headers and select the Column Preferences option
   1. Make sure you have Appearance -> Columns is selected
   2. Click the + at the bottom of the dialog box twice
   3. Double click the title of the first New Column and Name it Src Port
   4. Click the Type column and select Source Port (unresolved)
   5. Double click the title of the second New Column and Name it Dest Port
   6. Click the Type column and select Destination Port (unresolved)Destination Port (nonresolve)
   7. Left click Src Port and drag it under the Source column
   8. Left click Dest Port and drag it under the Destination column
   9. Click OK
   10. Right click the Src Port column and then click Align Left
   11. Right click the Dest Port column and then click Align Left
7. Click View -> Time Display Format -> UTC Date and Time of Day
8. Find the first packet having HTTP and in the Packet Details Pane expand Hypertext Transfer Protocol then right click Host: xxxxxxxxxxxxx and then Apply as Column

**Take a screen shot of your formatted Wireshark display and paste it below.**

**Graphical user interface, application

Description automatically generated**

1. Now that we have our display setup, let’s investigate. We know that, based on the alerts, we are interested in web traffic between 139.199.184.166 and 10.12.25.101. Let’s take what we know about the malicious traffic and filter it to only the applicable traffic. Enter ip.addr == 139.199.184.166 && ip.addr==10.12.25.101 && tcp.dstport==80 && http. This will filter the traffic to only traffic of interest.

**Take a screen shot of your filtered Wireshark display and paste it below.**

**Graphical user interface, table

Description automatically generated**

1. Scroll through the filtered data, noticing in the Info column we see requests for several different web pages. All of these web pages are requested by the same source IP address and are requested in quick succession. This is the behavior of a web vulnerability or attack scanner like Burp or Zap. Click the Statistics -> HTTP -> Requests. Notice that the host 128.199.64.235 many requests from different pages and with a number having a lot of special characters. Note: The host in the HTTP request will show the requested NAT/Public IP address available from the network while the packet capture shows the internal IP address of 10.12.25.101. This is normal for a NAT host that uses port forwarding.

**Take a screen shot of your formatted Wireshark display and paste it below.Graphical user interface, application

Description automatically generated**

We can plainly see based on the traffic that our web server using a private IP of 10.12.25.101 and a NATed public IP of 128.199.64.235. The host 139.199.184.166 used some type of web vulnerability/attack scanner to probe our web server.

Part 2 - Malware

In this next PCAP, we will look for malware. A single alert received by a security tool indicated that a user on the 10.8.19.0/24 LAN segment, on the domain funkylizards.com has been infected with malware. The domain controller for Funkylizard-DC is 110.8.19.8 and the LAN segment broadcast address is 10.8.19.255.

1. Start by opening the CYBR 440 - Shortcut folder on the Desktop then then navigate to Malicious Pcaps. Then open the 2021-08-19-traffic-analysis-exercise-alerts.pcap. Doubling click the file should open Wireshark and load the pcap file.
2. We know that the infected host is on 10.8.19.0/24. Lets start by opening the menu Statistics -> Endpoints. Next select the tab IPv4. The tap shows (60) meaning that 60 distinct IP addresses have been detected in this PCAP. Examining the Addresses we see the following IP addresses on the LAN, 10.8.19.1, 10.8.19.8, 10.8.19.101, 10.8.19.254, and 10.8.19.255. We know that 10.8.19.255 is the broadcast address so we can exclude that IP. 10.8.18.254 has only one packet recorded so we can exclude that. 10.8.19.1 only has 78 packets and is probably the default gateway/router so we can exclude that. 10.8.19.8 is the domain controller and we are interested in a workstation, so the only IP that has traffic of interest would be 10.8.19.101. Let’s filter out the traffic we don’t care about using this filter: ip.addr==10.8.19.101.

Table

Description automatically generated

1. Now that we have filtered out packets of interest, let’s see if we can collect information about the host. First open Statistics -> Protocol Hierarchy. This page show all of the different types of protocols captured in this traffic in a hierarchy. It looks like useful protocols for this investigation could be NetBIOS Name Service, DNS, SMB, Kerberos, and Hypertext Transfer Protocol. Let’s start by finding the name of the workstation. Right click the NetBIOS Name Service under User Datagram Protocol and select Apply as Filter -> …and Selected. This shows all the network traffic with Windows Netbios Name traffic. Packets with Info lines ending in <20> represent the hostname. Examine the packet list pane and find the hostname.

**Record the Hostname Below**

**Funky Lizards**

1. Now replace the (nbns) that was added to the filter with Kerberos.CNameString so your filter should now look like (ip.addr==10.8.19.101) && Kerberos.CNameString. Hit enter. On the first shown packet that shows AS-REQ in the info column, expand Kerberos in the packet detail, then req-body, then cname, then cname-string. Right click the CNameString and then select Apply as Column. The CNameString will show computer accounts ending in a $. Normal user accounts do not end in a $. Which user account was being used on 10.8.18.101?

I could not find the ip address 10.8.18.101 but for the ip address 10.8.19.101 is desktop-m1tfhb6$.

Graphical user interface, text, application

Description automatically generated

**Record the username below.**

PRINCIPAL

1. Delete && Kerberos.CNameString from the filter and hit enter, then open Statistics -> Protocol Hierarchy. Usually malware is delivered either via e-mail (SMTP,POP3,IMAP) or via the Web (HTTP,HTTPS). Since we only seem to have web traffic, right click Hypertext Transfer Protocol and select Apply as Filter -> … and Selected. The list of traffic is small, but we do see what looks like a single file download. In the Info column we see GET /ooiwy.pdf HTTP/1.1. Since this file download took place during the capture, we should be able to get this file out of the PCAP. Select File -> Export Objects -> HTTP. Select the line having the ooiwy.pdf file and then save. Save the file in the Malicious PCAP directory using the default name.

Graphical user interface, text

Description automatically generated

1. Using Windows File Explorer, navigate to the C:\CYBR 440\Malicious Pcaps\ folder. Right click on an empty area of the window while holding Shift and select Open PowerShell window here.

Graphical user interface, application

Description automatically generated

1. In the PowerShell window the appears, type Get-FileHash .\ooiwy.pdf. Make sure the SHA 256 hash that appears matches the following: F25A780095730701EFAC67E9D5B84BC289AFEA56D96D8AFF8A44AF69AE606404.Graphical user interface, text, application

   Description automatically generated
2. Using a computer that has Internet access, search for the SHA256 on VirusTotal. You can visit the VirusTotal Search page here: <https://www.virustotal.com/gui/home/search>. Paste in the SHA 256 hash from this document and press enter.

**What does Malwarebytes classify this file as?**

**Malwarebytes claims this is undetected but other vendors claims this is a Trojanhorse.**

**Search for this specific malware and write a short paragraph on this malware. What does it do? How does it spread? Why did the malware authors write it?**

*Ransomware* is a type of malware that encrypts the victim's files and demands a ransom payment to decrypt them. Ransomware can spread through email attachments, malicious websites, and USB drives. The malware authors write ransomware because they want to make money. They know that people will be willing to pay a ransom to get their files back.

*Ransomware* can be very damaging to businesses and individuals. It can cause data loss, downtime, and financial losses. It can also damage the victim's reputation. If you are infected with ransomware, it is important to act quickly. You should try to restore your files from a backup, if possible. If you do not have a backup, you may need to pay the ransom. However, it is important to remember that there is no guarantee that the ransomware authors will decrypt your files even if you pay the ransom.

1. This file ooiwy.pdf is a piece of real malware. It is a renamed DLL so you cannot run it by clicking on it directly, but because it is real malware, we will delete it. Click once on the ooiwy.pdf file to highlight it and then press SHIFT + DEL at the same time. This removes the file from disk without sending it to the Recycle Bin first. When Windows asks you if you are sure, you permanently want to delete file click yes.

Deleted.

Part 3 - Comparing Raw Packet Captures to NetFlow and Firewall Logs

Now that have some experience looking at raw packet captures, lets go back and look at NetFlow and firewall filter logs.

1. Close Wireshark and open a browser. 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#!! where # is your student/analyst number.
2. On the search tab, enter filterlog into the search bar and press enter or the search button. Examine the information provided with the firewall filter log. Make sure you click on one of the filter logs to see the details.
3. On the search tab, enter NetFlowV9 into the search bar and press enter or the search button. Examine the information provided with the NetFlow v9 records. Make sure you click on one of NetFlow logs to see the details.

Answer the following questions

**What is the difference in detail captured between NetFlow, firewall logs, and raw packet captures?**

The main difference in detail captured between NetFlow, firewall logs, and raw packet captures is that NetFlow and firewall logs provide high-level information about traffic, while raw packet captures provide detailed information about individual packets.

**Which would be more useful in investigating malware?**

Raw packet captures

**Which types of network logs/capture would take more storage space?**

Raw packet captures would take more space than NetFlow or firewall logs. This is because raw packet captures capture the entire contents of each packet on the network, while NetFlow and firewall logs only capture a summary of the traffic.

**What kinds of things could firewall and NetFlow logs be useful for over raw packet captures?**

*Identifying trends and patterns:* Firewall and NetFlow logs can be used to identify trends and patterns in network traffic. This information can be used to identify potential security threats, such as denial-of-service attacks or malware infections.

*Troubleshooting problems:* Firewall and NetFlow logs can be used to troubleshoot problems with the network. For example, if you are having trouble accessing a particular website, you can use the firewall logs to see if there are any blocked packets.

*Compliance:* Firewall and NetFlow logs can be used to comply with regulations, such as those set by the Sarbanes-Oxley Act or the Payment Card Industry Data Security Standard. These regulations require organizations to maintain logs of network traffic for a certain period.

*Forensics:* Firewall and NetFlow logs can be used in forensics investigations. For example, if there has been a security breach, you can use the logs to identify the source of the breach.