**Name: Nwachukwu Edumanichukwu**

**CYBR 440 - Incident Detection and Response  
Module 5 Lab – Acquiring Host-Based Evidence and Forensic Imaging of Memory**

In this fifth 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 at <https://workspace.bellevue.edu>. 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 your three analyst tools you will use throughout this course.

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

Part 1 - Local Memory RAM Capture

In this first lab, we will take a memory image from a Windows 10 system locally. Memory images, unlike disk images, are used to capture a point-in-time snapshots of running processes and are often used for malware analysis (as we will see in the Module 6 lab).

1. Open a new connection to RDP Workstation# in a new tab.
2. After logging in, navigate to C:\CYBR 440. You can do this using Windows Explorer or clicking on the Desktop shortcut to CYBR 440. Then navigate to WinPMEM.

Graphical user interface, application

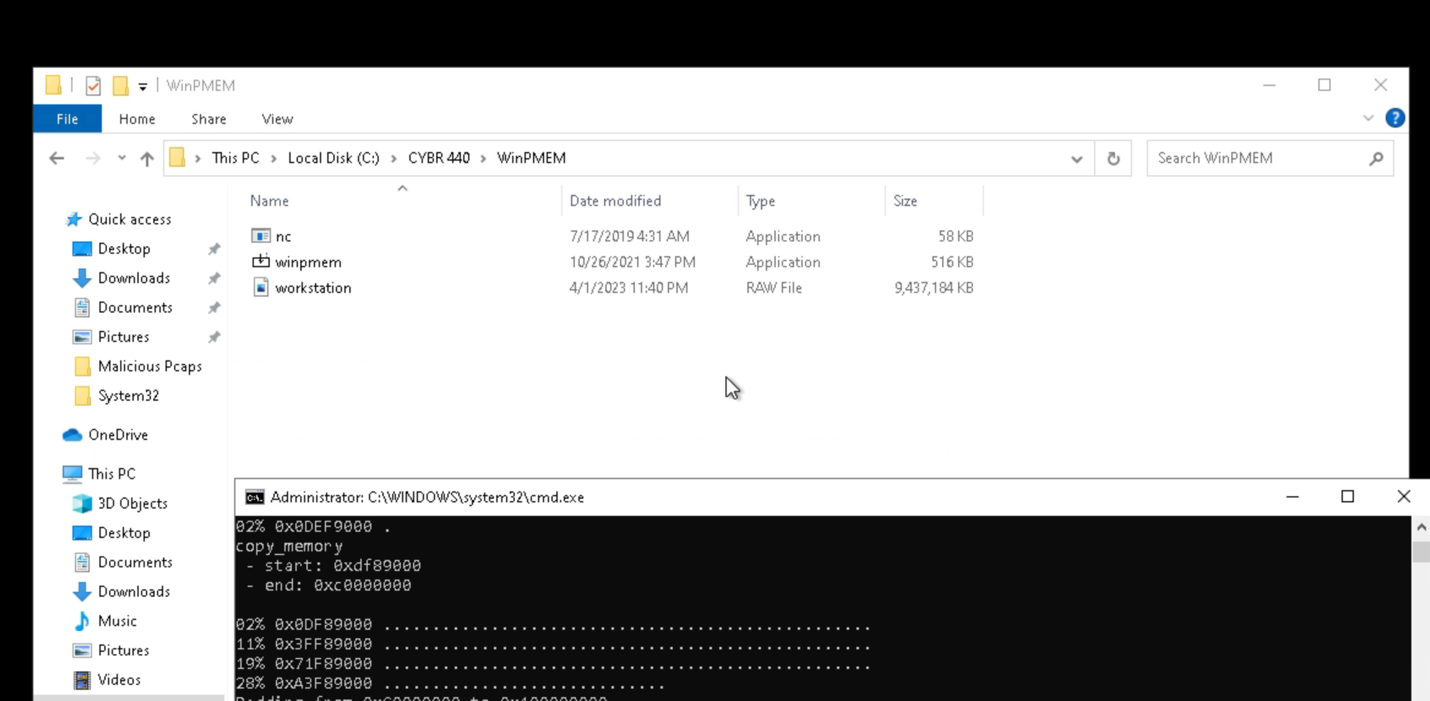
Description automatically generated

1. While holding SHIFT, right click the background Windows Explorer in the WinPMEM folder then select Open command window here.

Graphical user interface, text, application

Description automatically generated

1. Now run the command winpmem workstation.raw. It will take several minutes for this command to finish.

**Take a screenshot of the folder with the workstation.raw image file in it and paste it below**

Part 2 - Remote RAM Capture

In this second part we will start a new ram capture from a remote Linux (Kali) system. The process is the same as the previous RAM capture with the exception being we will be sending the RAM capture to a remote system instead of a local file.

1. Keep your existing tab to Workstation # open. Go back to the remote management connection list tab. Right click the link to SSH Kali # and open it in a new tab.
2. In the Kali SSH tab, type nc -nvlp 4445 > workstation.raw
3. In the Windows 10 Workstation tab, go to your open command line window from the previous and run the following command: winpmem - | nc 172.28.37.91 4445. The command will appear to freeze, but it is transferring the RAM capture over the network in the background.
4. After a few minutes, navigate to the Kali SSH tab and press CONTROL+C. This will stop the command from running. Transferring RAM over the network can take a long time and we will stop this RAM capture early so we can move on to other tasks.
5. type ls -l in the Kali SSH window

**Paste a screenshot of the previous command belowText

Description automatically generated**

Part 3 - Installing and Configuring Windows Auditing and Advanced Audit Policy

By default, the Windows logs are not very good sources of information for detecting malicious software and other types of attacks. To correct this, we will modify the default Windows logging settings and then install Sysmon with a configuration tailored to detecting attacks.

1. Go to the desktop of your Windows 10 Workstation and double click the gpedit.msc shortcut.
2. Navigate to Computer Configuration -> Windows Settings -> Local Policies -> Security Options.

A picture containing text

Description automatically generated

1. Change Audit: Audit the access of global system objects to: Enabled then click Apply.
2. Change Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings to: Enabled and then click Apply.
3. Now navigate to Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies - Local Group Policy Object

Timeline

Description automatically generated

1. Under System Audit Policies - Local Group Policy Object, change the following settings
   1. Account Login
      1. Audit Credential Validation - Failure
      2. Audit Kerberos Authentication Service - Success, Failure
      3. Audit Kerberos Service Ticket Operations - Failure
      4. Audit Other Account Login Events - Success, Failure
   2. Account Management
      1. Audit Application Group Management - Success
      2. Audit Computer Account Management - Success
      3. Audit Distribution Group Management - Success
      4. Audit Other Account Management Events - Success
      5. Audit Security Group Management - Success
      6. Audit User Account Management - Success, Failure
   3. Detailed Tracking
      1. Audit PNP Activity - Success
      2. Audit Process Creation - Success
   4. DS Access
      1. Audit Directory Service Access - Failure
      2. Audit Directory Service Changes - Success
   5. Login/Logoff
      1. Audit Account Lockout - Failure
      2. Audit Group Membership - Success
      3. Audit Logon Success - Failure
      4. Audit Other Login/Logoff Events Success - Success, Failure
      5. Audit Special Logon - Success
   6. Object Access
      1. Audit Detailed File Share - Failure
      2. Audit File Share - Success, Failure
      3. Audit Other Object Access Events Success, Failure
      4. Audit Removeable Storage - Success, Failure
   7. Policy Change
      1. Audit Audit Policy Change - Success
      2. Audit Authentication Policy Change - Success
      3. Audit MPSSVC Rule-Level Policy Change - Success, Failure
      4. Audit Other Policy Change Events - Failure
   8. Privilege Use
      1. Audit Sensitive Privilege Use - Success, Failure
   9. System
      1. Audit Other System Events - Success, Failure
      2. Audit Security State Change - Success
      3. Audit Security System Extensions - Success
      4. Audit System Integrity - Success, Failure
2. After you are done making these change, right click the Desktop while holding SHIFT and select Open command window here.
3. In the command window, type the command gpresult /H report.html. This command will take a few minutes to create a HTML report of the computer’s security settings.
4. When the command has finished running, close the command prompt window.
5. Open the Settings -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Configuration entry in the report.
6. Open every item under Advanced Audit Configuration. You should see a list of changes you recently made to the audit configuration.

**Paste a screenshot of the settings in the report. You do not have to show all the settings, but you should show as many as you can fit into the screen.Table

Description automatically generated**

Part 4 - Installing Sysmon with Tuned Configuration

As mentioned in Part 3, Windows is not very good at logging the things that helps us detect attacks. One further change we can make to improve Windows logging is to install Sysmon with a configuration that allows us to log additional items to the Windows event log. The configuration we will use for this exercise is found here: <https://github.com/SwiftOnSecurity/sysmon-config>.

1. Close the report.html document you had open, if it is still open, then click CYBR 440 on the desktop or navigate to C:\CYBR 440\Symon.
2. Right click the empty folder while holding SHIFT and select Open command windows here.
3. Type the command sysmon64.exe -accepteula -i sysmonconfig-export.xml. If the command is successful, you will see the following lines:
   1. Loading configuration file with schema version 4.50
   2. Sysmon schema version: 4.81
   3. Configuration file validated.
   4. Sysmon64 installed.
   5. SysmonDrv installed.
   6. Starting SysmonDrv.
   7. SysmonDrv started.
   8. Starting Sysmon64..
   9. Sysmon64 started.

**Paste a screenshot of the successful command being run below.Text

Description automatically generated**

Part 5 - Forwarding Windows logs to the Graylog SIEM

Now that we have captured RAM and configured Windows for robust logging, we will want to forward the logs to a central SIEM. We will be using a log forwarder called NXlog to forward our logs to Graylog. With this configuration, we can search through and analyze logs from many systems from one central location. It also keeps attackers from deleting evidence as they must gain access to the original computer and the SIEM to delete logs.

1. Navigate to the Desktop then the CYBR 440 folder or C:\CYBR 440, then open the NXLog folder.
2. Double click the nxlog-ce-2.11.2190.msi NXLog installer.
3. On the Welcome to the NXLog-CE Setup Wizard dialog, click Next.
4. On the EULA page, click I accept the terms in the License Agreement and click Next.
5. On the Destination Folder dialog, click Next to accept the default installation path.
6. On the Ready to Install NXLog-CE dialog click Install.
7. When the install is finished, uncheck Open README.txt… and click Finish.
8. Now copy the C:\CYBR 440\NXLog\nxlog.conf file to C:\Program Files (x86)\nxlog\conf and overwrite the existing nslog.conf. If you want, open the nxlog.conf in notepad to see the configuration. It will forward all Windows event logs to Graylog using the GELF format.

**#Note: I did not see the nxlog.conf file in the C:\CYBR 440\NXLog.**Graphical user interface, text, application, email

Description automatically generated

1. Open the command line and run net stop nxlog then net start nxlog.
2. Log into graylog by opening Chrome and browsing to <https://graylog1.bbtrust.com:9000> then login using the username analyst# and the password An@lyst#!! where # is your analyst/student number.
3. Search for workstation#.bbtrust.com where # is you analyst/student number. Make sure your windows logs are being forwarded to Graylog.

**Paste a screenshot of your logs as shown in the Graylog search page.Graphical user interface

Description automatically generated with medium confidence**

**I was able to modify the nxlog.conf file in Program Files (x86) by changing the port number to get the log forwarded to greylog.**

Part 6 - Installing Elastic Endpoint Security EDR tool

In this lab we will install and check the operation of an EDR tool.

1. Open a browser on your RDP Workstation# and navigate to <https://elastic1.bbtrust.com:5601>. Login using the username analyst# and password of An@lyst#!!.
2. If you get prompted to add data, skip this step and start using Kibana by clicking Explore on my own.

Graphical user interface, application, Teams

Description automatically generated

1. Open the menu by clicking on the three parallel lines/hamburger on the upper left of the page. Scroll down to Management -> Fleet. Click on Fleet.

Graphical user interface, application

Description automatically generated

1. Make sure the Agents tab is selected. You should see one agent, elastic1.bbtrust.com. This is the Fleet server, the component that manages all other endpoints. Click the blue + Add agent, on the right side of the screen.
2. Make sure the Enroll in Fleet tab is selected. Scroll down to the 3. Enroll and start the Elastic Agent. Change the platform from Linux / macOS to Windows.
3. Copy the entire command shown below, starting with .\elastic-agent.exe install …. You can also click the stacked documents to the right of this command to copy the entire command.
4. From your Desktop, click the CYBR 440 folder, or in Windows Explorer, navigate to C:\CYBR 440. Open the Elastic Agent folder. Then open the Elastic Agent folder.
5. Right click on an empty area inside the folder while holding SHIFT and select the Open command window here option.
6. Paste the command you copied by right clicking the command prompt window, then press ENTER. The Elastic Agent installation may take a few minutes. You should see the following in the command prompt window if installation is successful.

Text

Description automatically generated

1. Return to your browser. The Elastic Fleet page should now show your workstation# or workstation#.bbtrust.com. Stay on this page and continuing watching until the Status of your workstation changes from Updating to Healthy.

Text

Description automatically generated with medium confidence

Graphical user interface, text, application

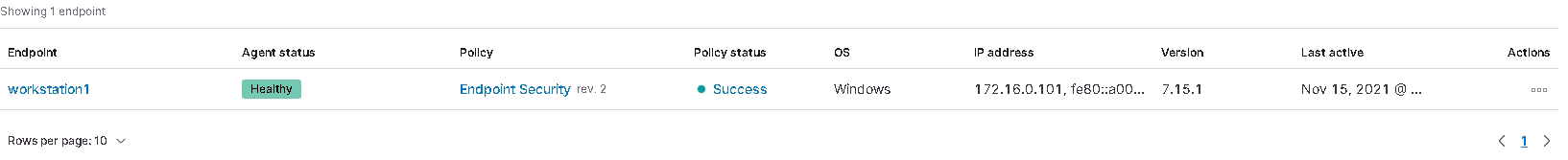
Description automatically generated

1. Open the three parallel lines/hamburger menu on the left side of the screen, scroll down and select Security -> Endpoints.

Graphical user interface, text, application

Description automatically generated

1. Wait for the Agent Status column of this table to change to Healthy. This may take a few more minutes as the security agent is a subcomponent of the endpoint agent.



1. Navigate back to your workstation # Desktop on then open the KnowBe4 Ransomware Simulator. After it opens, click the Check now button. You will see Elastic Agent Malware Alerts on the lower left of the screen. Let this simulator run to completion.
2. After the ransomware simulator has finished running, return to your browser and click on Alerts on the left side of the Security page.
3. At the top of the pages, where it says alerts, type host.name: “workstation#” where # is your analyst/student number. You should see several alerts with timestamps corresponding to when you ran the ransomware simulator. If these do not show up, wait a few minutes, and press the blue Refresh button until you see events.

**Take a screen shot of the page showing events for you workstation and paste it below.Graphical user interface, application

Description automatically generated**