**Nwachukwu Edumanichukwu**

**CYBR 440 - Incident Detection and Response  
Module 12 Lab – Threat Hunting**

In this twelve and final lab, we will look at threat hunting use a tool called Velociraptor. Velociraptor is based on the Google GRR Rapid Response, which allows you to do certain types of remote forensics via a central server and an agent. Threat hunting is the process of taking IOCs and other indicators and proactively searching for threat on your network before your normal controls prevent or alert on malicious behavior. We will use Velociraptor to remotely look for registry keys, network connections, files, and file hashes.

**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

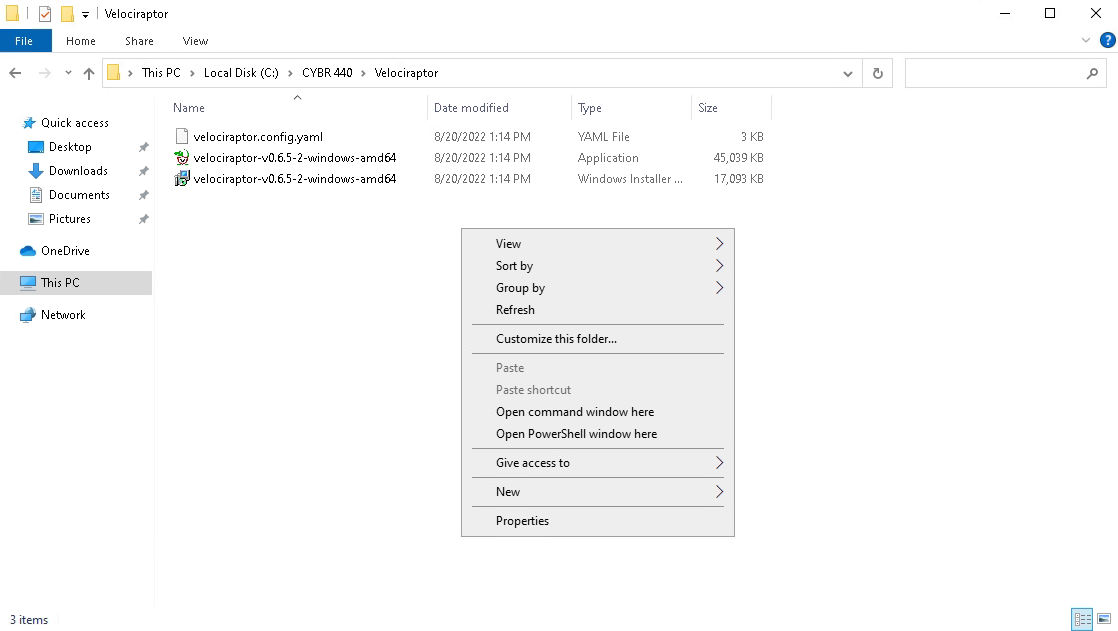
You should have three available connections, RDP Kali #, RDP Workstation#, and SSH Kali #. These are your three analyst tools you will use throughout this course.

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.

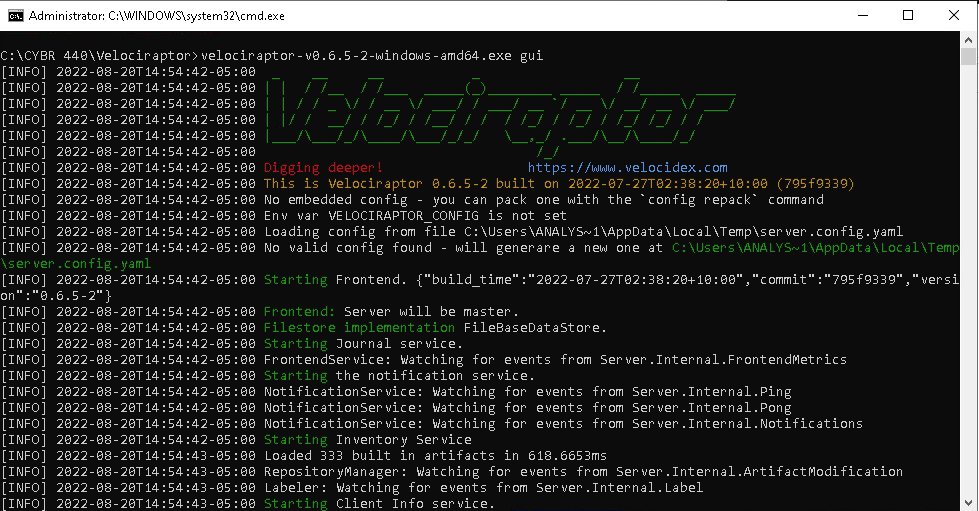
Part 1 - Threat Hunting with Velociraptor

This short lab shows you how to threat hunt using the Velociraptor digital forensics and incident response tool.

1. After accessing your analyst desktop via the management portal. Start a standalone instance of Velociraptor by navigating to C:\CYBR 440\Velociraptor. Open a command shell by right clicking Explorer and clicking “Open command window here.”



1. Start Velociraptor by type “velociraptor-v0.6.4-2-windows-amd64.exe gui”. This should start Velociraptor and start a web browser. Click Advanced and then Proceed to 127.0.0.1 (unsafe).



Graphical user interface, text, application, email

Description automatically generated

1. On the left side of the screen, select the Hunt button. It looks like a target reticle.



1. Click on the + on the top of the screen to start a new hunt. Fill out the following on the next screen.
   1. Description: Registry Hunt 6
   2. Expiry: Leave blank
   3. Include Condition: Run everywhere
   4. Exclude Condition: Run everywhere
2. Click on the Select Artifacts tab on the bottom of the page. At the top of the screen search for Power, then select Windows.System.Powershell.
3. On the bottom of the screen select Configure Parameters. In the Command textbox type Get-Item -Path Registry::HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run.
4. Click on the Specify Resources tab at the bottom of the screen. Examine this screen but leave all the values at their default values.
5. Click on Review. Examine the JSON file that specifies the hunt to be run. You can craft the Hunt requests by simply specifying the JSON if you want to do something custom.
6. Select the Launch tab on the bottom of the screen. The hunt will be ready to launch but will begin in the paused state. Select your Hunt in the table and then click the Play button. On the dialog Run this hunt? Click Run it! Wait for the Finished clients to display 1.
7. Click on the Download Results dropdown and Summary (CSV Only). Click the -summary link that appears. You will download the file in .zip. Open the .zip file and then open the All Windows.System.PowerShell.csv file.

**What two program are run on startup according to the results?**

**Security Health and VMWare User Process**

**Paste a screenshot of the CSV. You can open the results in the editor of your choice.A screenshot of a computer

Description automatically generated with low confidence**

1. Click on the + on the top of the screen to start a new hunt. Fill out the following on the next screen.
   1. Description: Network Connections Hunt 6
   2. Expiry: Leave blank
   3. Include Condition: Run everywhere
   4. Exclude Condition: Run everywhere
2. Click on the Select Artifacts tab on the bottom of the page. At the top of the screen search for Power, then select Windows.Network.NetstatEnriched
3. On the bottom of the screen select Configure Parameters. Click the wrench next to Windows.Network.NetstatEnriched. In the IPRegex field, replace the default value with 172\.28\.37\.2[12]. This searches for the IP addresses 172.28.37.21 and 172.28.37.22. These are the management servers that make remote connections using RDP to your analyst workstation. This will show you all active RDP connections for all students.
4. Click on the Specify Resources tab at the bottom of the screen. Examine this screen but leave all the values at their default values.
5. Click on Review. Examine the JSON file that specifies the hunt to be run. You can craft the Hunt requests by simply specifying the JSON if you want to do something custom.
6. Select the Launch tab on the bottom of the screen. The hunt will be ready to launch but will begin in the paused state. Select your Hunt in the table and then click the Play button. On the dialog Run this hunt? Click Run it! Wait for the Finished clients to display 1 Overview tab.
7. Click on the Download Results dropdown and Summary (CSV Only). Click the -summary link that appears. You will download the file in .zip. Open the .zip file and then open the All Windows.System.PowerShell.csv file.

**What is the issuer name and Subject name certificate associated with the RDP server on the analyst workstations?**

Issuer name: " "C=U5, ST=Washington, L-Redmond, O-Microsoft Corporation, CN-Microsoft Windows Production PCA 2011" "

Subject name: " "C=U5, ST=Washington, L=Redmond, O=Microsoft Corporation, CN-Microsoft Windows Publisher" "

**Take a screenshot of the data associated with your analyst workstation connection to the management server. The data will start with a PID and end with the hostname workstation#.bbtrust.com. The data is multiline and includes MD5, SHA1, and SHA256 hashes.A close-up of a computer code

Description automatically generated with low confidence**

1. Click on the + on the top of the screen to start a new hunt. Fill out the following on the next screen.
   1. Description: File Hunt 9
   2. Expiry: Leave blank
   3. Include Condition: Run everywhere
   4. Exclude Condition: Run everywhere
2. Click on the Select Artifacts tab on the bottom of the page. At the top of the screen search for Power, then select Windows.Search.FileFinder.
3. On the bottom of the screen select Configure Parameters. Click the wrench next to Windows.Search.FileFinder. In the SearchFileGlob enter C:/KnowBe4/RsSimulator/\*.exe. This is the directory that has the ransomware simulator installed. Click the trashcan icon next to SearchFileGlobTable to delete C:/Users/SomeUser/\*.
4. Click on the Specify Resources tab at the bottom of the screen. Examine this screen but leave all the values at their default values.
5. Click on Review. Examine the JSON file that specifies the hunt to be run. You can craft the Hunt requests by simply specifying the JSON if you want to do something custom.
6. Select the Launch tab on the bottom of the screen. The hunt will be ready to launch but will begin in the paused state. Select your Hunt in the table and then click the Play button. On the dialog Run this hunt? Click Run it! Wait for the Finished clients to display 1 Overview tab.
7. Make sure your file hunt is selected and then click to the Notebook tab. If no data is displayed, click within the Notebook tab to bring up an additional menu then click the Recalculate button. Examine the results in this HTML table and answer the questions below.

**What three executables are found in the C:\KnowBe4\RsSimulator directory?**

**Collector.exe, Ranstart.exe, Start.exe**

**Take a screenshot of the results table under the Notebook tab and paste it below.A close-up of a computer screen

Description automatically generated with low confidence**

1. Click on the + on the top of the screen to start a new hunt. Fill out the following on the next screen.
   1. Description: Hash Hunt # where # is your student/analyst number
   2. Expiry: Leave blank
   3. Include Condition: Run everywhere
   4. Exclude Condition: Run everywhere
2. Click on the Select Artifacts tab on the bottom of the page. At the top of the screen search for Power, then select Generic.Forensics.LocalHashes.Glob.
3. On the bottom of the screen select Configure Parameters. Click the wrench next to Generic.Forensic.LocalHashes.Glob. In the HashGlob enter C:/KnowBe4/RsSimulator/\*.exe.
4. Click on the Specify Resources tab at the bottom of the screen. Examine this screen but leave all the values at their default values.
5. Click on Review. Examine the JSON file that specifies the hunt to be run. You can craft the Hunt requests by simply specifying the JSON if you want to do something custom.
6. Select the Launch tab on the bottom of the screen. The hunt will be ready to launch but will begin in the paused state. Select your Hunt in the table and then click the Play button. On the dialog Run this hunt? Click Run it! Wait for the Finished clients to display 1 on the Overview tab.
7. Make sure your hash hunt is selected and then click to the Notebook tab. If no data is displayed, click the Recalculate button. Examine the results in this HTML table and answer the questions below.

**Which executable has the hash d833eff67a923b26785211fd46c01de3?**

**Ranstart.exe**

**Paste a screenshot of the results table below.A picture containing text, screenshot, algebra

Description automatically generated**

1. At the top of the page, in the textbox that says, Search clients, enter the name workstation# where # is your student/analyst number, and then press the search button. On the next page it should show your analyst workstation hostname. Click on the blue Client ID next to your hostname.
2. The next page that comes up shows a summary of your analyst workstation. Hover over the button with a brief case with a medical symbol. This button isolates the host from the network except for Velociraptor traffic. This is a common function for EDR and distributed forensics tools.
3. Click the VFS button. This brings up a virtual file, folder, and registry browser. Click on NTFS the click on the folder icon with a R next to it. This fetches the list of file and directory names from your analyst workstation and allows you to interactively browse the filesystem remotely. The client will take a few minutes to sync the filesystem to the Velociraptor server.
4. Navigate to ntfs -> \\.\C: -> KnowBe4 -> RsSimulator. If at any point you see No data available. Refresh directory from client by clicking above. Click the folder button with the R next to it. Select Ranstart.exe and examine the stats in the details pane.

**Take a screenshot of the VFS page showing Ranstart.exe selected and the detailed stats and paste it below.A screenshot of a computer

Description automatically generated with low confidence**

1. On the left menu on the side of the page, select the Notebook icon. This is where we document the results of a complete investigation.



1. Select the + to create a new notebook. Name it Analyst # Notebook. In the description enter Test Investigation. Click Submit.
2. Click on the text below where it says Analyst # Notebook until you see a menu bar appear. Click the plus on the rights ide of the menu and then select Add Cell from hunt then Registry Hunt # where # is your student/analyst number.

Text, whiteboard

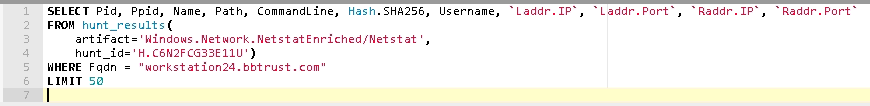
Description automatically generated

1. In the new cell that is added, click the edit button having a pencil icon and add WHERE Fqdn = “workstation#.bbtrust.com” under the FROM clause as shown below. Click the save button. The table should now only show the results from your analyst workstation in the table.

Text

Description automatically generated

1. Click on the cell having the newly added information from your registry hunt until you see a menu bar appear. Click the plus on the right side of the menu and then select Add Cell from Hunt. Select Network Connections Hunt # where # is your student/analyst number.
2. In the new cell that is added, click the edit button having a pencil icon and add WHERE Fqdn = “workstation#.bbtrust.com” under the FROM clause as shown below. Click the save button. The table should now only show the results from your analyst workstation in the table. Make sure you are using backticks under the escape key for quoting items with a period after the SELECT.



1. Click on the cell having the newly added information from your network connections hunt until you see a menu bar appear. Click the plus on the right side of the menu and then select Add Cell from Hunt. Select File Hunt # where # is your student/analyst number.
2. In the new cell that is added, click the edit button having a pencil icon. In this VQL we will modify the query to find out how many .exe files in C:\KnowBe4\RsSimulator we have across all our endpoint. Modify the query to change SELECT \* to SELECT FullPath, count() as Number. Add a WHERE command under the FROM clause that reads WHERE FullPath =~ “.\*exe$”. Change the LIMIT 50 to GROUP BY FullPath. See below.

Text

Description automatically generated

1. Click on the cell having the newly added information from your file hunt until you see a menu bar appear. Click the plus on the right side of the menu and then select Add Cell from Hunt. Select Hash Hunt # where # is your student/analyst number.
2. In the new cell that is added, click the edit button having a pencil icon. In this VQL we will modify the query to find out which workstation have a certain hash in C:\KnowBe4\RsSimulator we have across all our endpoints. Modify the query to change SELECT \* to SELECT Fqdn, FullPath, Hash. Add a WHERE command under the FROM clause that reads WHERE Hash = “d833eff67a923b26785211fd46c01de3. Change the LIMIT 50 to ORDER BY Fqdn. See below.

Text

Description automatically generated