**Cybersecurity 401**

**Module 7 - Threat Hunting**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Lab 31 - Threat Hunting with YARA**

## 

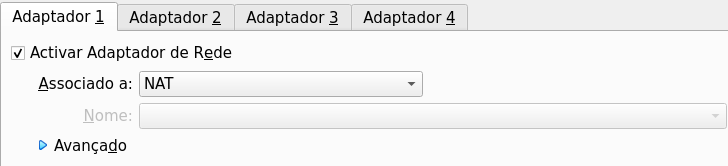
**| Rodrigo Brasil 12/2023 |**

### **Part 1: Staging**

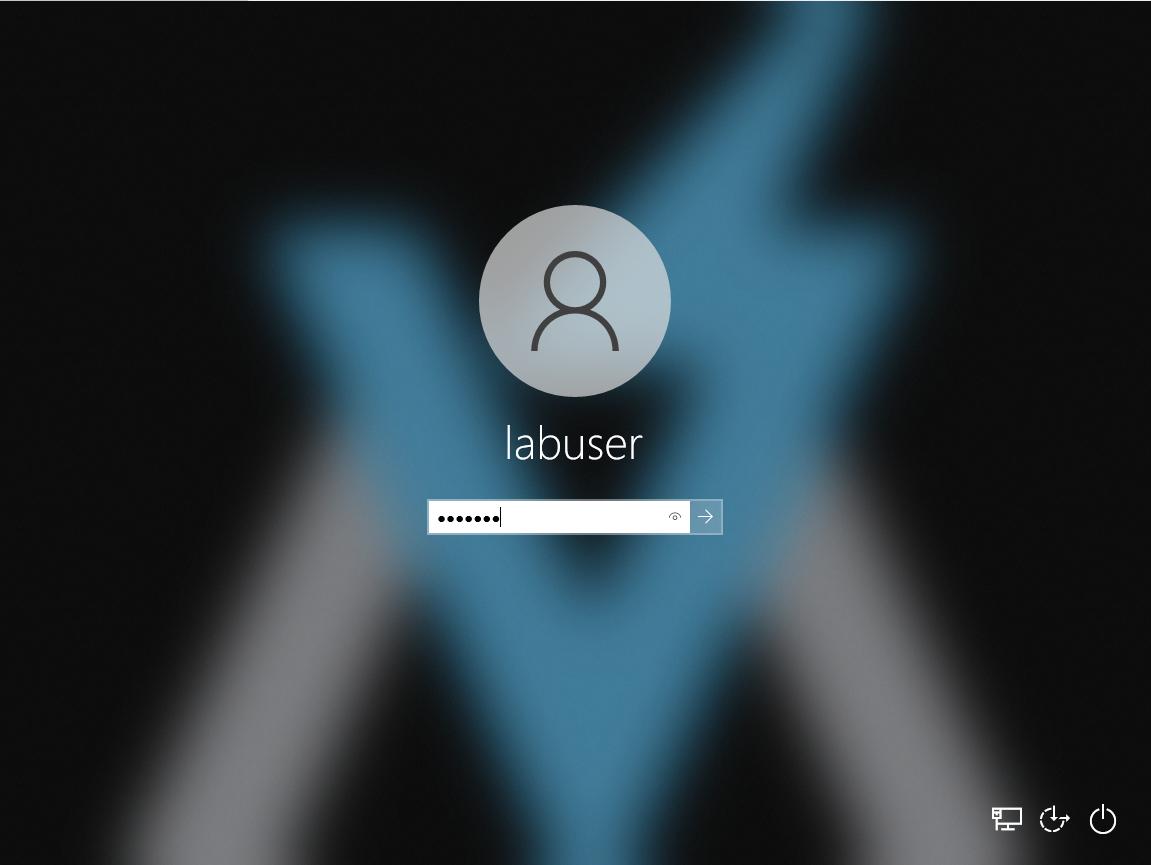
* **Download and import the Flare VM OVA.**

****

* **Set the network adapter to NAT Network.**

****

* **Login as labuser / labuser.**

****

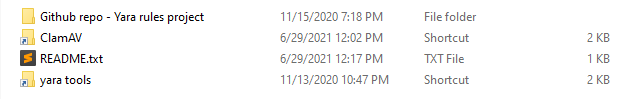
**Password is: labuser**

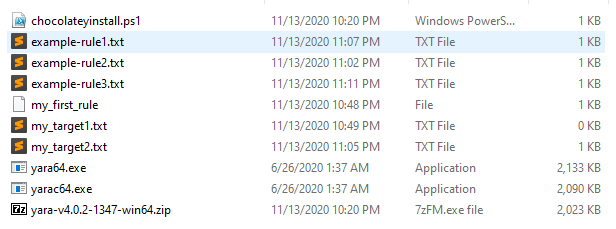
### 

### **Part 2: My First YARA Rule**

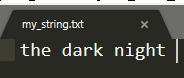
* **Access the “yara tools” folder on the desktop. This shortcut will take you to the directory where yara64.exe is installed. You’ll need to call yara64.exe from command line to use it.**

****

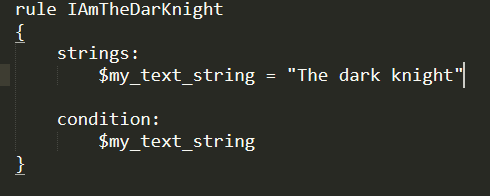
****

****

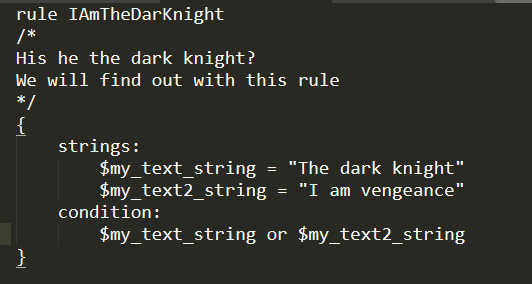
* **Create a text file containing a string of your choosing.**

****

* **Create a YARA rule that tests whether the target file contains the string of your choosing.**

****

* **Include comments in your YARA rule.**

****

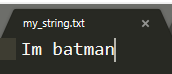
* **Execute the YARA rule against the target file.**

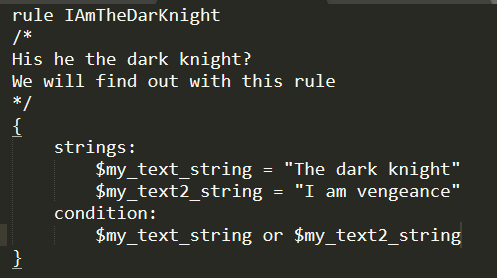
****

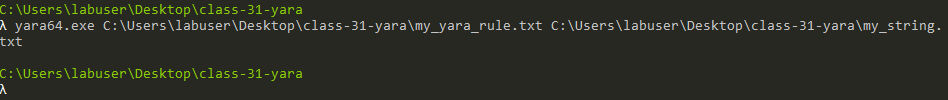
* **Include a screenshot of the YARA rule and its output.**

****

* **Explain whether the rule tested positive or negative. How can you tell?**
  + **It tested positive because it matched with the string in the my\_string.txt file and the output gave me the name of my rule**
* **Create a file that does not contain your string. Run your rule against it to generate a negative. Note the difference in output.**

****

****

****

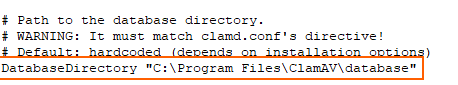
### 

### **Part 3: Customizing ClamAV with YARA Rules**

* **Run Fresh Clam to pull the latest virus signatures database into ClamAV’s database directory. You may need to edit the configuration files in ClamAV directory to facilitate the process.**

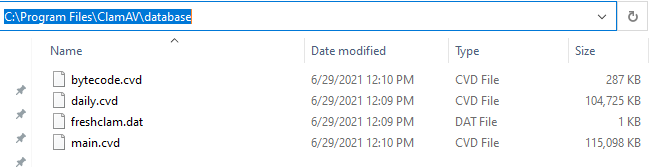
****

****

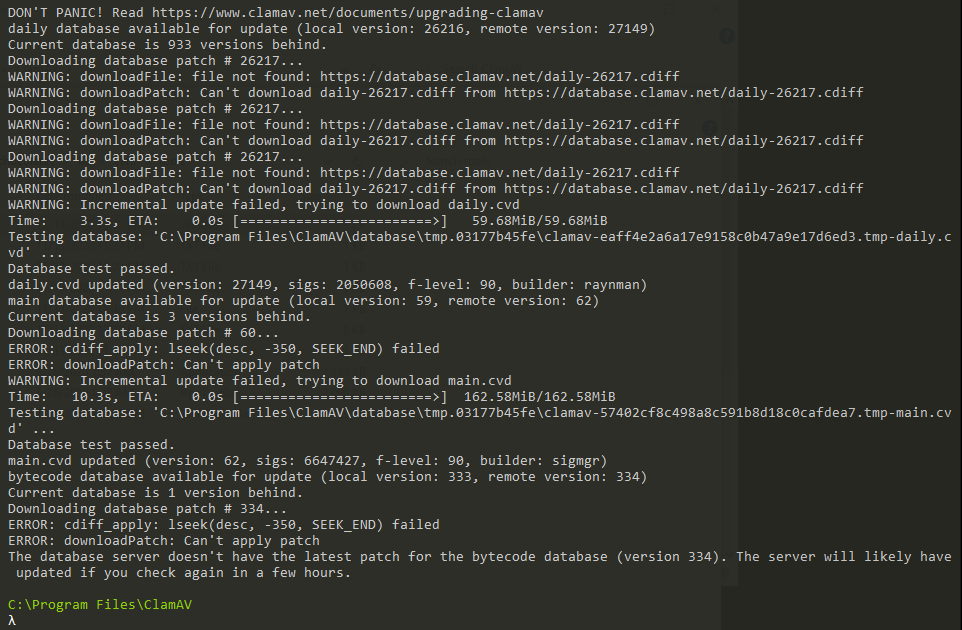
****

****

****

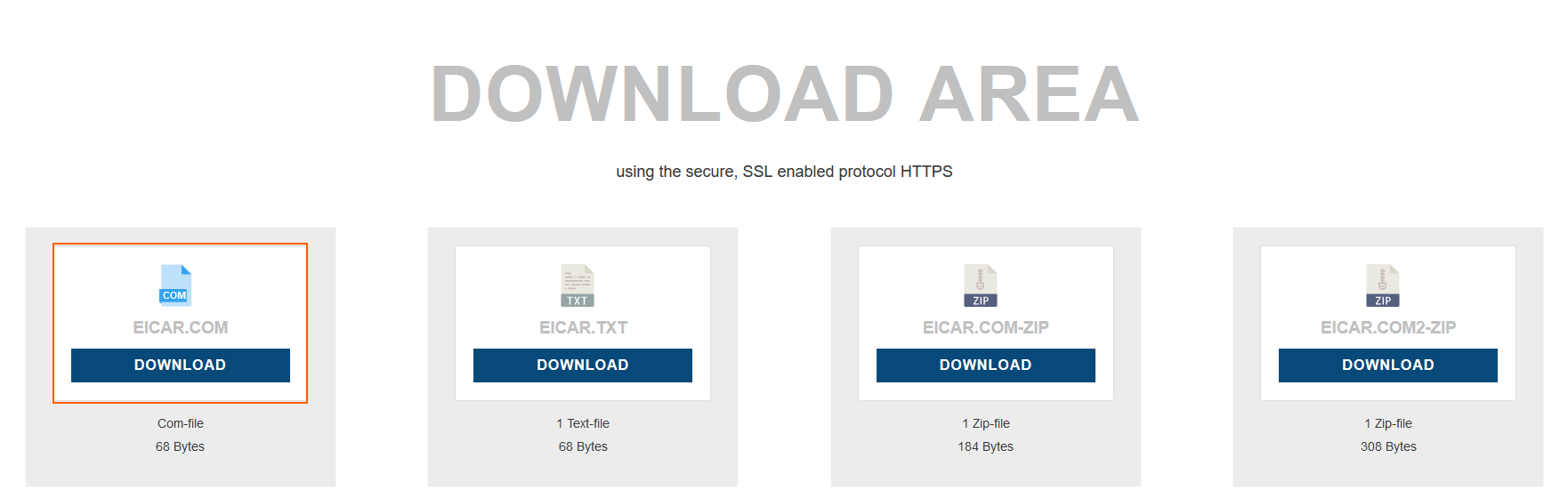
****

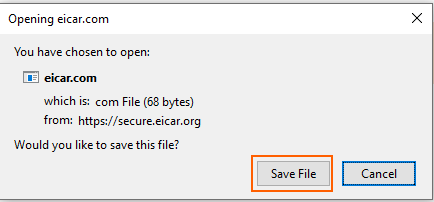
****

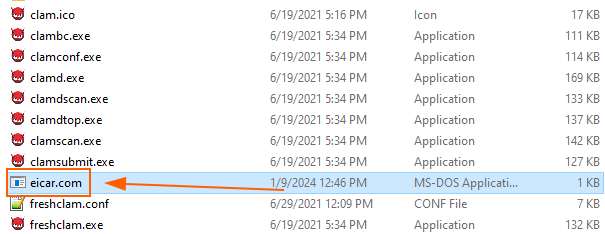
****

* **Practice running ClamAV to perform a scan against the eicar.com file in the ClamAV directory.**
  + **eicar.com wasn't on my directory ClamAv maybe because of windows defender so i manually downloaded the file from here: https://www.eicar.org/download-anti-malware-testfile/**

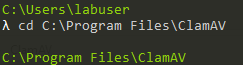
****

****

****

****

**After downloading, put it in the ClamAv directory**

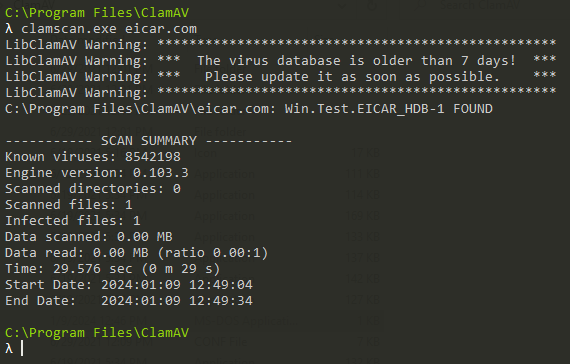
****

**on the terminal when to the directory**

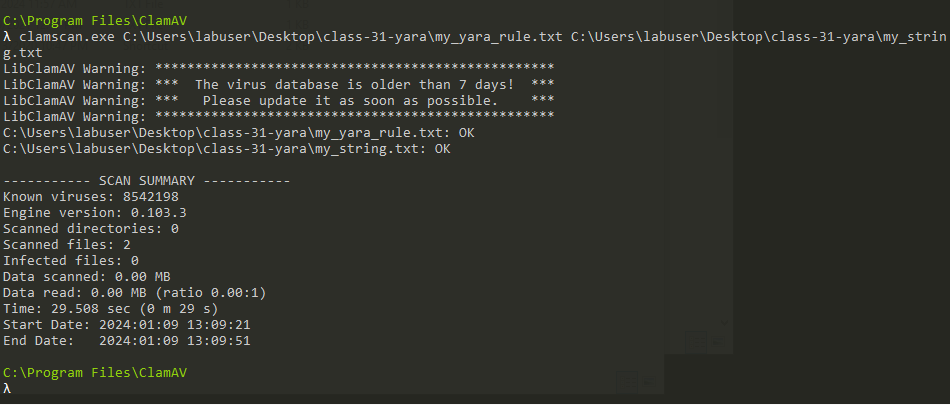
****

**and ran the scan against it**

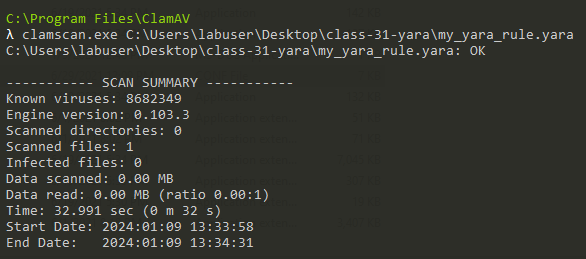
* **Include a screenshot of the positive detection.**

****

* **Use ClamAV to scan your target text file from Part 2 using the rule you created in Part 2. Do this by instructing ClamAV to use your YARA rule instead of its signature database. Include a screenshot and explanation of how you achieved this.**

****

* **Next, instruct ClamAV to scan the target text file from Part 2 using both the rule we created and ClamAV’s signature database. Include a screenshot and explanation of how you achieved this.**

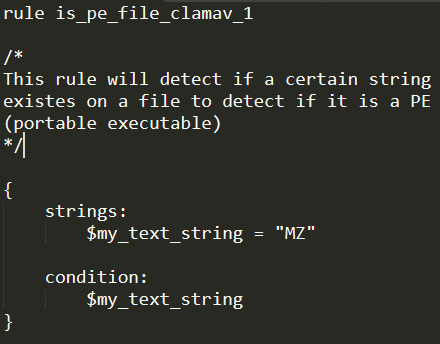
****

**PE files contain the string “MZ”. Let’s create a rule that determines whether the target is a PE file.**

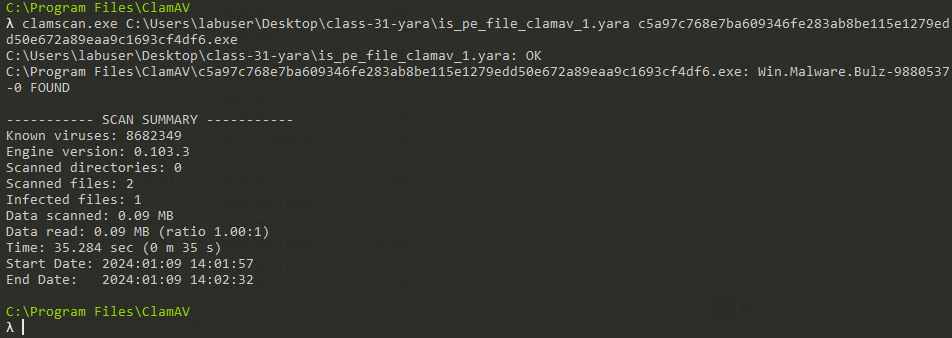
* **Create a new YARA rule named “is\_pe\_file\_clamav\_1.yara”.**

****

* **Write the rule to look for the string “MZ” in its target.**

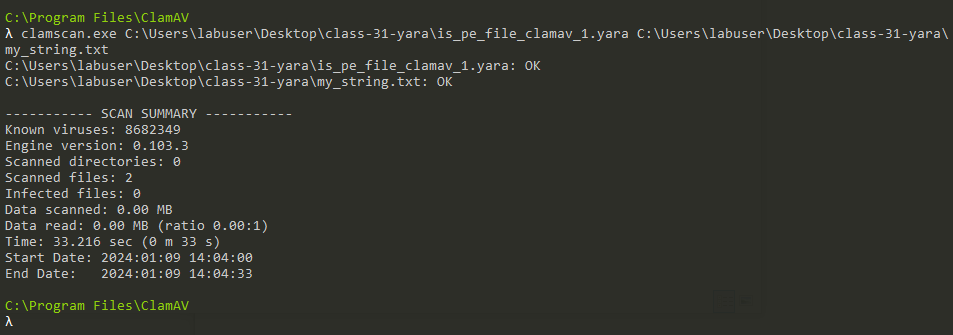
****

* **Test the rule using ClamAV against a PE file and a non-PE file. Include screenshots and discussion.**

****

**PE file**

**I downloaded a sample PE malware from** [**https://bazaar.abuse.ch/**](https://bazaar.abuse.ch/) **and from the result it identified it as an infected file because inside it it has the MZ string of the created rule.**

****

**non-PE file**

**In this scan I simply ran the rule against a txt file that I created with the simple frase “I am the dark knight” . From the scan, because there was no MZ string it did not identify any infected files.**

### 

### **Part 4: Reporting**

**Answer the below prompts to the best of your ability:**

* **What else can YARA detect?**
  + **Yara can also detect hashes, URL’s, registry changes and more**
* **What if you don’t have a single string to search for in the target?**
  + **it can still search for other characteristics patterns or behaviors like searching for a file sizes or a line of code**
* **How would you explain ClamAV’s “file decomposition” feature?**
  + **It employs techniques such as file type recognition, archive extraction, heuristic scanning, and PE file analysis to analyze the content and structure of files for potential threats.**