Lab 2: Implementation of Prometheus into Ashburn’s Frog Emporium’s Integrated Defense in Depth Strategy

**Security Team:** Luis Ruiz, Marcos Vallejos, Ryan Rockett, Kari Hattabaugh

Table of Contents

[Introduction 2](#_Toc84194081)

[Scope 2](#_Toc84194082)

[Information About Prometheus 4](#_Toc84194083)

[Prerequisites 4](#_Toc84194084)

[Installation, Configuration, and Testing Instructions 5](#_Toc84194085)

[Recommendations 12](#_Toc84194086)

[Alternatives 13](#_Toc84194087)

[Conclusion 14](#_Toc84194088)

[Sources 15](#_Toc84194089)

# Introduction

Ashburn’s Frog Emporium is interested in implementing an integrated defense in depth system into their business’s information security. Their security team’s goal was to identify and implement a tool to automatically monitor and alert the user of unusual or malicious network activity. With a lower budget and customizability in mind, the security team implemented the Prometheus toolkit. The team also explored the Splunk tool and highly recommends this tool if the organization is open to a monthly subscription service, as Splunk offers a great deal of options as well as support from their company.

# Scope

Ashburn’s Frog Emporiumis a small scale amphibian dealer, which does business online and in a brick and mortar location. While they maintain a store front and breed all animals on site, the online sales bring in a majority of their revenue. With the evolving world of information technology, there is a growing need for internet facing companies. With the goal of protecting their assets and customers, Ashburn’s Frog Emporium has hired a security team to build a budget conscious and user friendly information security system. This organization primarily uses Windows 10 workstations and Windows 2016 servers. The security team has identified that the most effective type of defense includes an integrated defense in depth, which places tools throughout a network to manage the different layers of a defense. Each of these layers are listed below with a brief description of each.

Previously, the security team implemented a free tool called Wireshark, a packet capturing software which allows a user to capture some network traffic and explore the different types of traffic on a network. This can be used to identify any unusual network activity with some additional training for the user. This tool satisfies the Network Auditing and log Files layer of the integrated defense in depth model.

The next tool to be implemented is Prometheus, a free monitoring and alerting toolkit. This tool allows the user to design their own network monitoring metrics. Metrics are used to determine whether an alarm should be set off based on network activity. This allows for automated monitoring throughout the network looking for malicious or unusual activity. Additionally, Prometheus’s alerts can be logged to keep a record of malicious or unusual activity. This tool offers a solution to both the Intrusion Detection and Prevention Systems and the Network Auditing and Log Files layers.

|  |  |  |
| --- | --- | --- |
| **Layer** | **Description** | **Tools Applied** |
| Physical Security | Measures taken to protect a computer or other network device from theft, fire, or environmental disaster. |  |
| Authentication and Password Security | Password policies, identity verification, etc. |  |
| Operating System Security | Maintaining and managing OS patches |  |
| Antivirus Protection | Protection the network and connected devices from malware. |  |
| Packet Filtering | Blocking or allowing the transmission of packets based on configured criteria. |  |
| Firewalls | The tools installed and configured to manage traffic on a network, including firewall policies. |  |
| Demilitarized Zone (DMZ) | The area on the exterior of the network, which focuses on accessibility and the network’s perimeter security. |  |
| Intrusion Detection and Prevention Systems (IDPS) | Technology used to detect and in some cases produce an automated response to signatures, or patterns on suspicious network activity. | Prometheus |
| Virtual Private Network (VPN) | Technology that allows for secure communication using public internet connection. |  |
| Network Auditing and Log Files | Recording and organizing network activity and performance to allow for analytics. | Wireshark, Prometheus |
| Routing and Access Control Methods | Tools that control or limit movement into and throughout the network. |  |

# Information About Prometheus

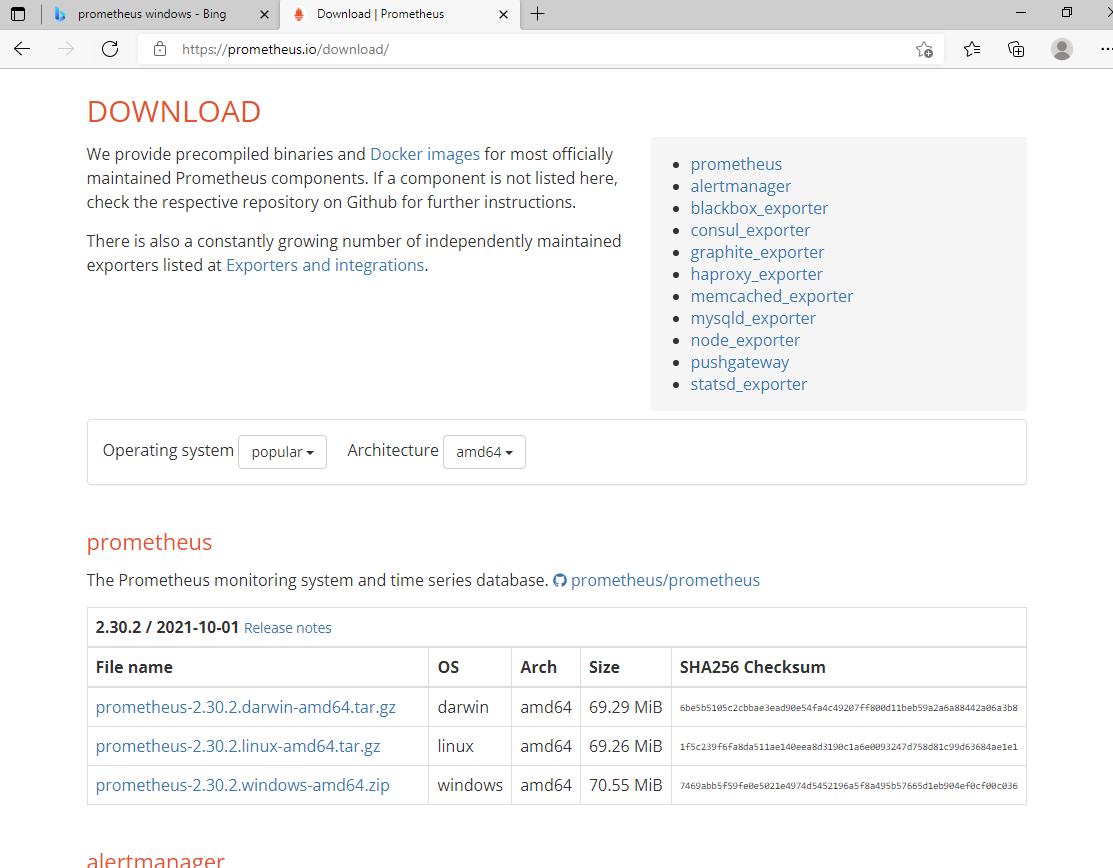
As mentioned previously, our team has decided to implement Prometheus, a free software application used for event monitoring and alerting. This toolkit will allow users to construct the metrics necessary for setting up alerts and the monitoring of events occurring on the network. The application Prometheus is available for free, is open source with an active user community, and has been adopted in many organizations such as AT&T, OneMain Financial, and JPMorgan Chase. Prometheus gathers metrics from different systems across the network by scraping data from HTTP endpoints. It uses this information to identify issues, such as when an endpoint is missing or when a time-series pattern indicates a problem.

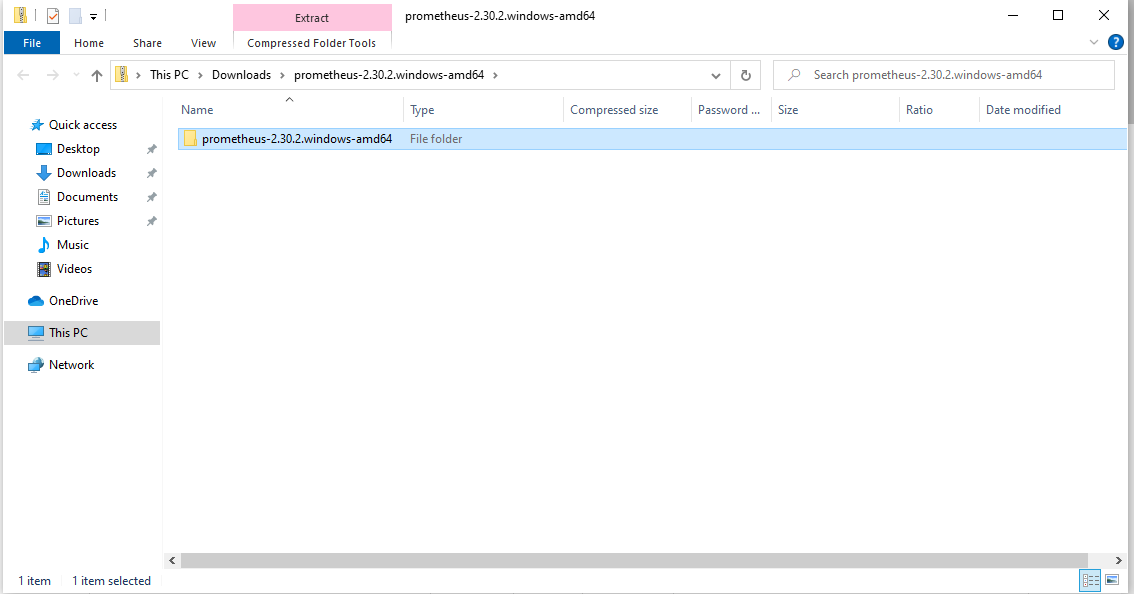
Prometheus monitors application metrics like throughput (TPS) and response times. Users can use the Node exporter to monitor host hardware and kernel metrics. The application has a local on-disk time-series database, which stores information with a default retention time of 15 days. It also integrates with remote storage systems. The metrics collected by Prometheus provide insights into the performance of our systems throughout the network, as well as notifying security events and unusual activity.

## Prerequisites

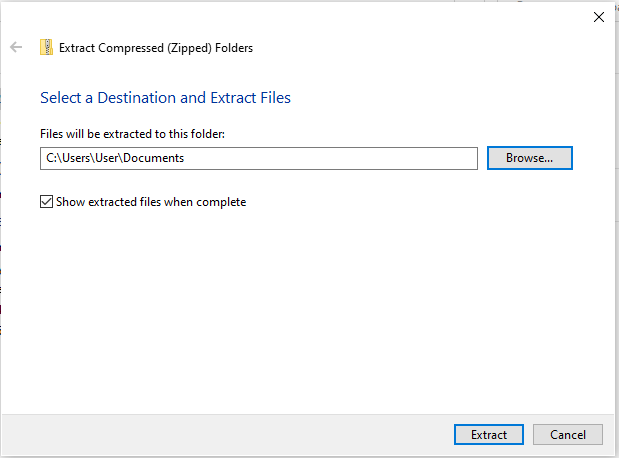
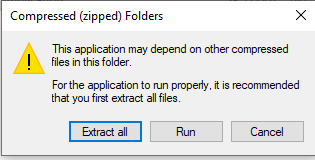
1. Before installing Prometheus, you must first check the workstations’ operating system. For our network, we will need to install the Prometheus software for our Windows 10 workstations.
2. Prometheus will support the following systems:
   1. Windows 10
   2. Windows Server 2016
3. Processor required:
   1. 64-bit AMD64 - Required by the 64-bit version being installed
4. At least 2 GB of usable RAM
5. At least 10 GB of local disk storage

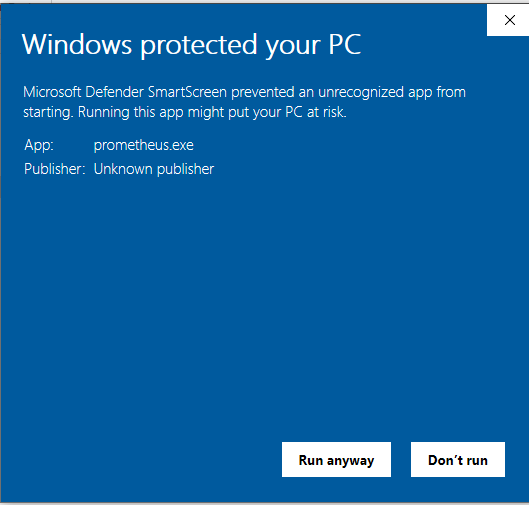
## Installation, Configuration, and Testing Instructions

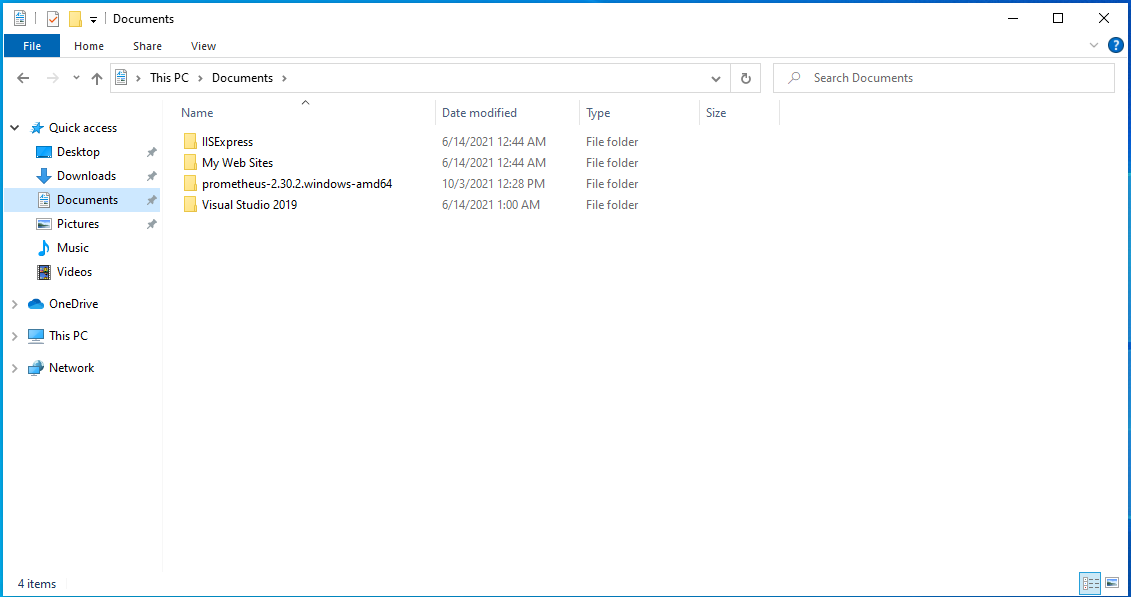
1. Boot up Windows10 device and open an internet browser. In this case we used Microsoft Edge, however Google Chrome and Mozilla Firefox would be acceptable options. Navigate to https://prometheus.io/download/. You should see the screen shown below. There are various versions of Prometheus and OS options available, we will be choosing the latest version which is [prometheus-2.30.2.windows-amd64.zip](https://github.com/prometheus/prometheus/releases/download/v2.30.2/prometheus-2.30.2.windows-amd64.zip) for OS. 
2. A compressed zip file will be created in your downloads folder.



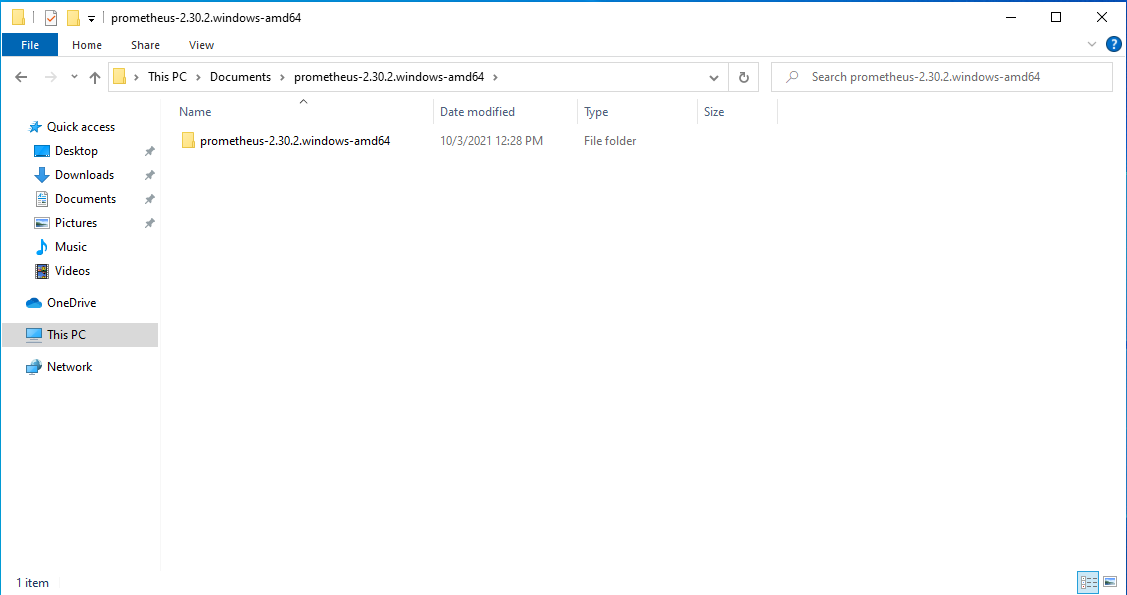
1. You will then have to extract that file into a location where you will be able to maintain it. We have moved it to our documents folder however, any other folder where it will be secured is possible.



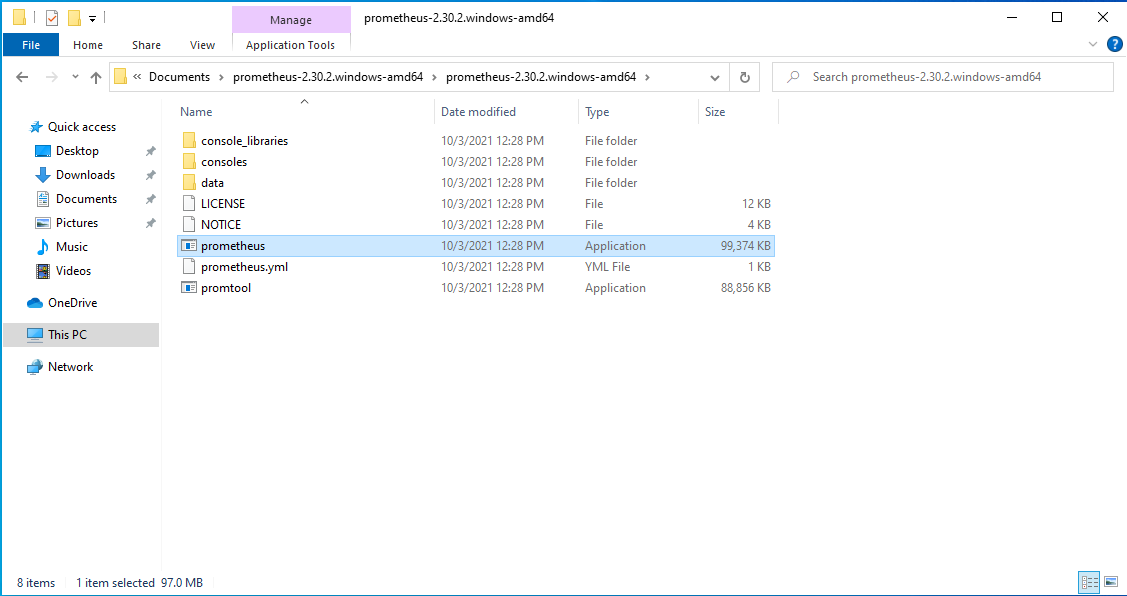
1. Windows will then show a prompt that it has prevented the application from running. We have confirmed that this application is safe to run. Click Run Anyway. 
2. You will now see a folder with the extracted files. We have it in our documents folder but make sure that you remember where you have located the folder for yourself.

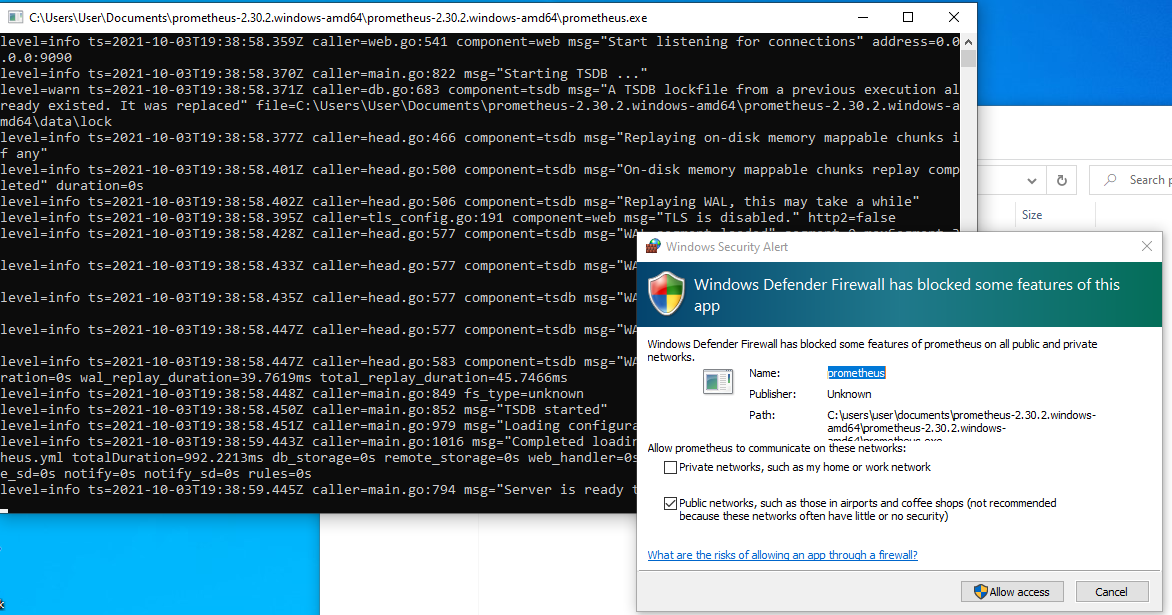


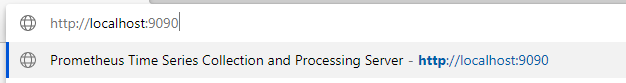
1. Click the folder labeled as [prometheus-2.30.2.windows-amd64](https://github.com/prometheus/prometheus/releases/download/v2.30.2/prometheus-2.30.2.windows-amd64.zip)

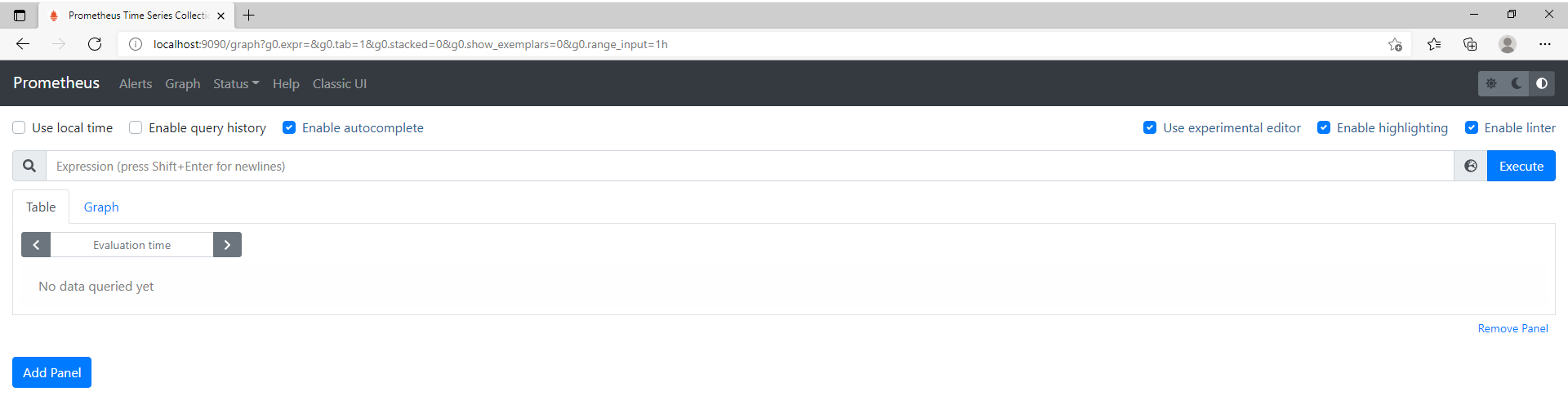
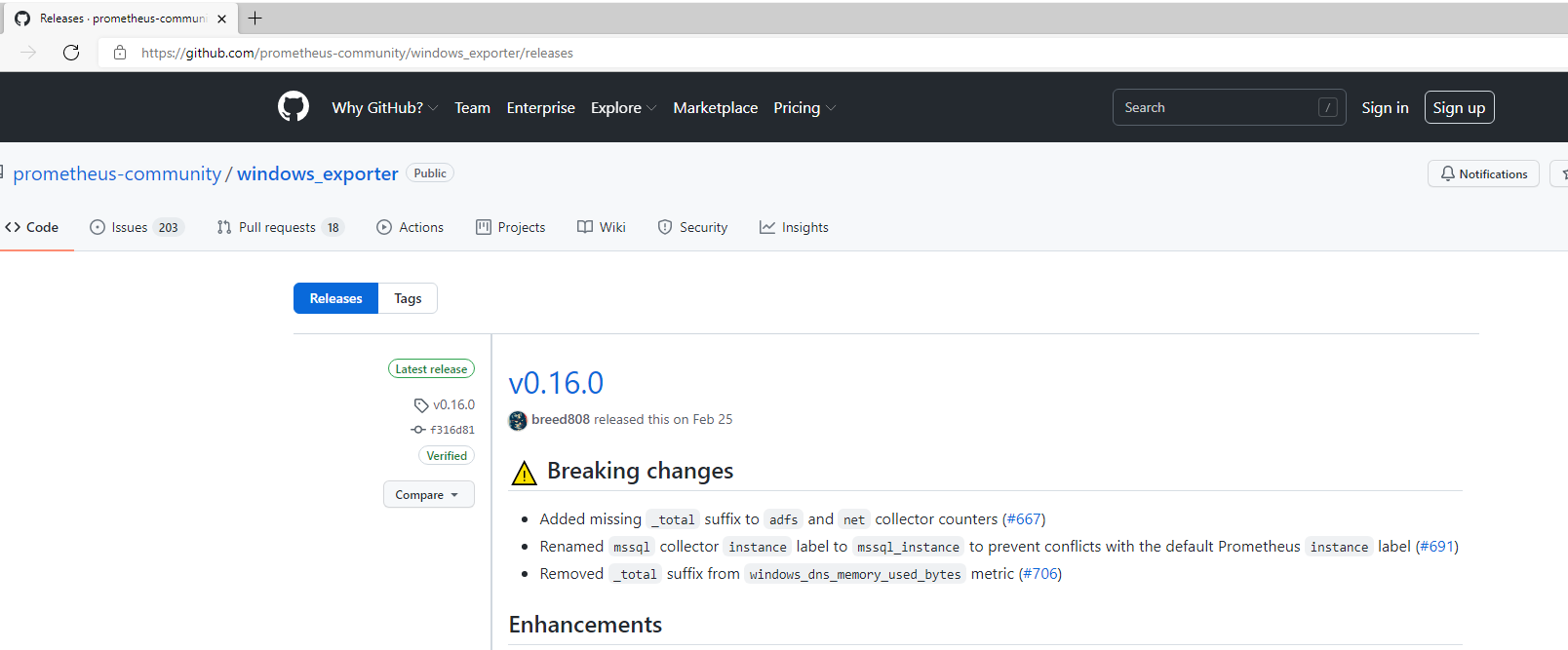
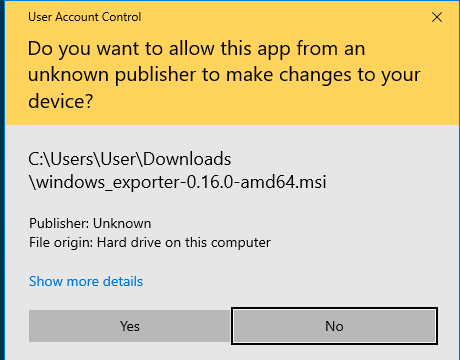
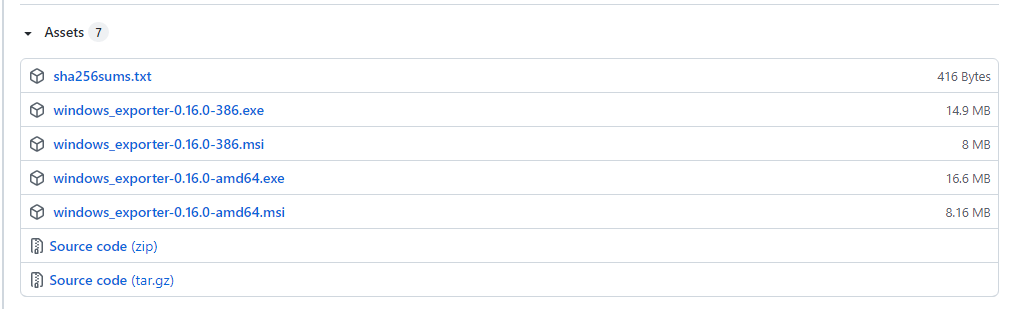
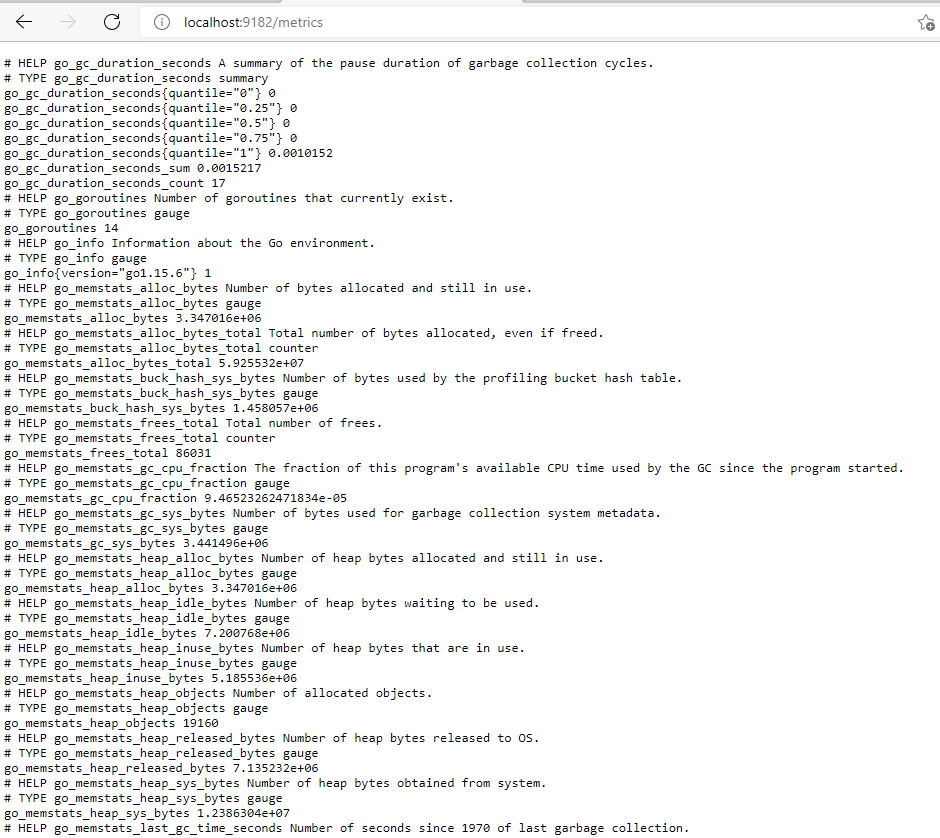
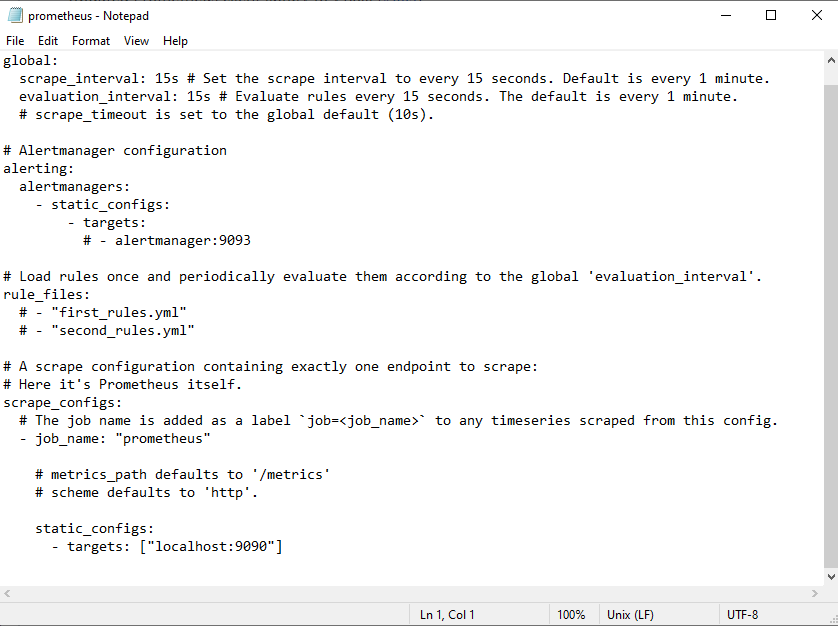
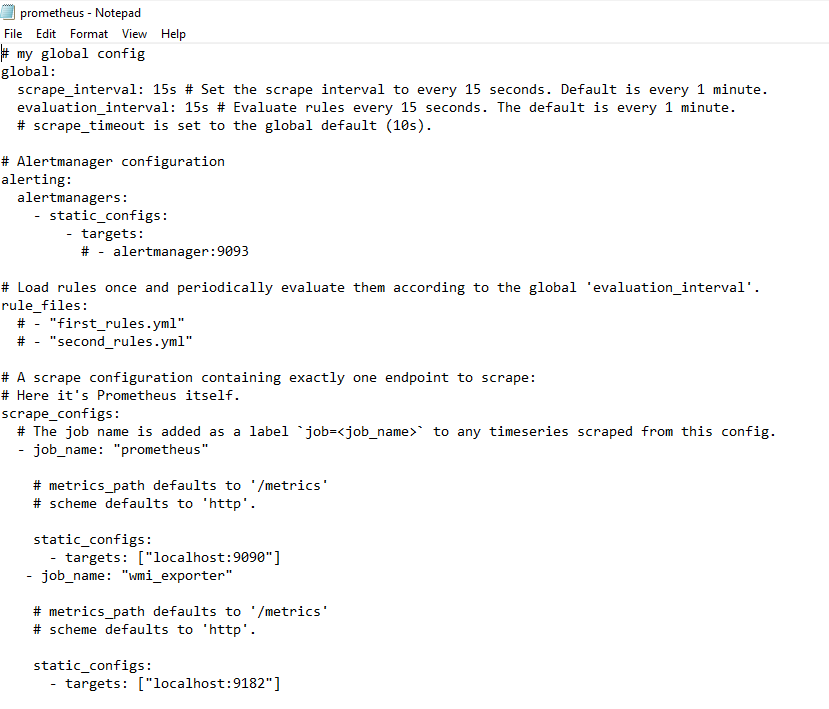
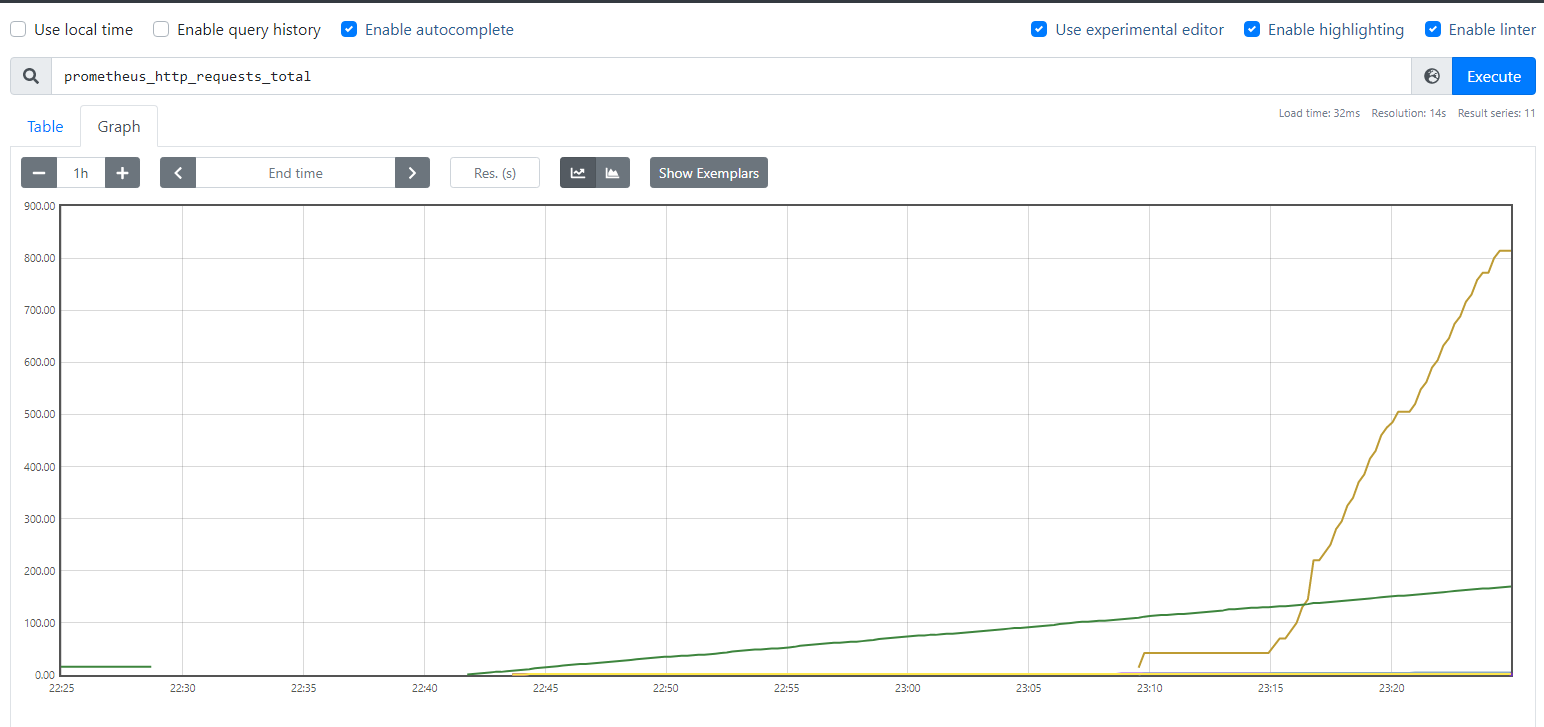
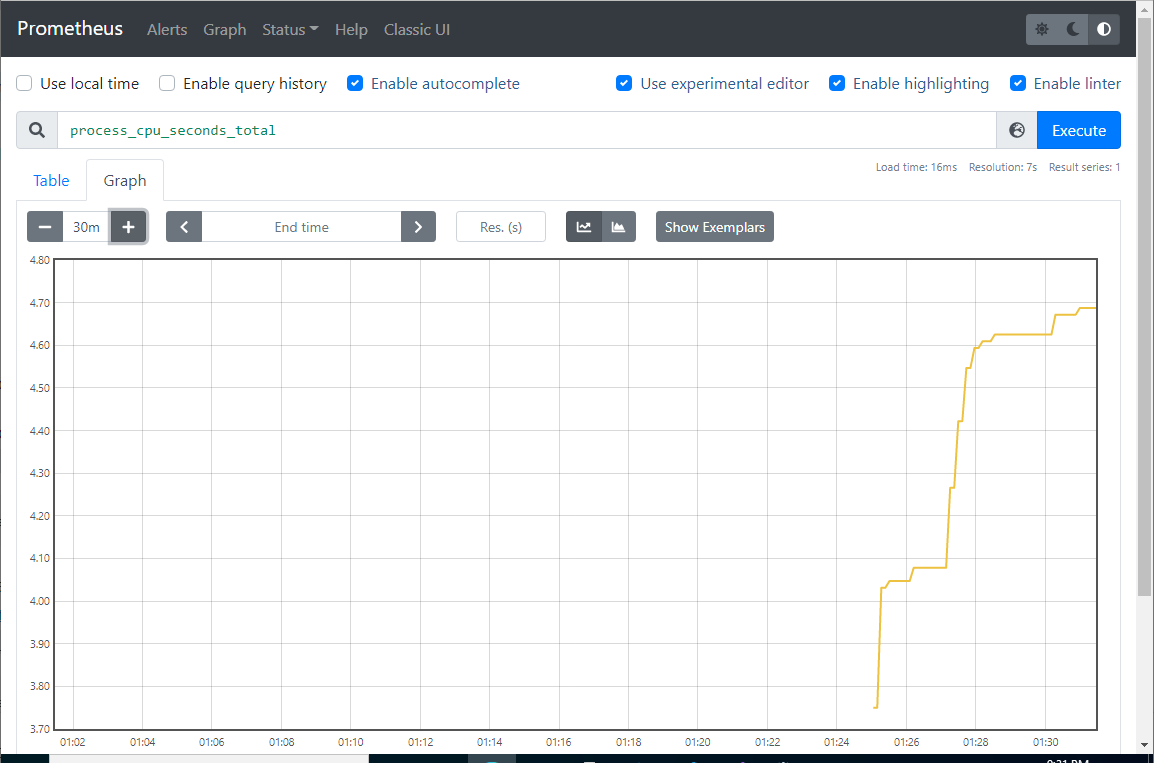


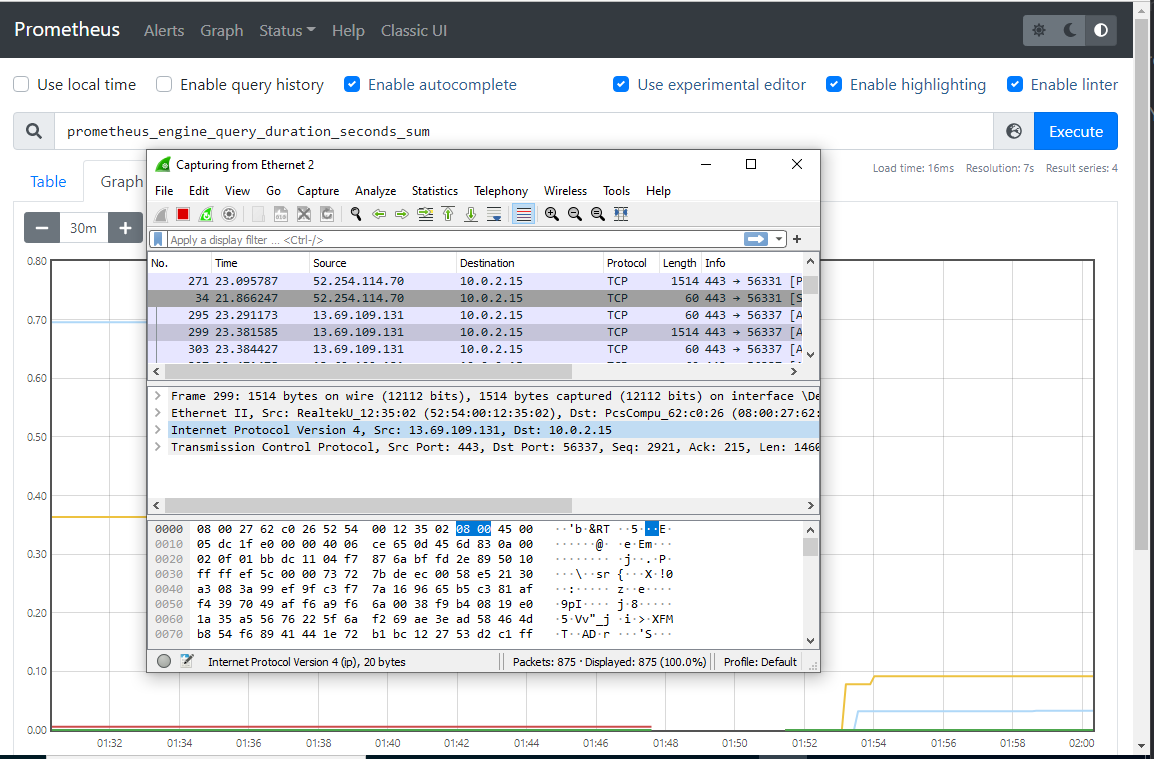
1. In this folder you will see the prometheus executable command, and the prometheus.yml file. For now, we will focus on the executable file and then we will come back to the .yml file later. Click on the prometheus application.



1. Windows firewall will block the application from running, click allow access through the firewall. If you do not allow access to the application, then we will not be able to monitor our traffic or proceed with further implementations that use Prometheus as a base. It is crucial to allow it access through the firewall, we need the application to be running in the background.
2. The Prometheus server will use port 9090. In order to use the application, we will go to a browser and type localhost:9090 this will take us to the Prometheus dashboard.



1. The dashboard will allow us to use expressions to monitor our networks as a base component.
2. Now we will download windows export to Prometheus. This will provide us with metrics for the CPU, System, OS, Network Interfaces, Memory, Hardware and logical disk. Navigate to <https://github.com/prometheus-community/windows_exporter/releases>.
3. There are various options but we will choose [windows\_exporter-0.16.0-amd64.msi](https://github.com/prometheus-community/windows_exporter/releases/download/v0.16.0/windows_exporter-0.16.0-amd64.msi)
4. We have also verified that this application is secure. Allow it access to make changes to our device.
5. Once it is finished installing, it will close itself without notification. Navigate to localhost:9182/metrics on your browser. To verify that it is operating correctly we will navigate to port 9182, if it is installed, we will see the following display.
6. Next, we will configure windows exporter as a target with prometheus so that it can display the metrics that windows exporter is able to access. This is another crucial step that will be necessary when we begin to integrate other tools with prometheus. To do this, we will navigate to the folder holding the prometheus.yml file. We will see the following when we open the file. 
7. We will be adding port “9182” as a target prometheus. To do this, in the open file we will create the job name, set the defaults then set the static configuration target to “localhost:9182” as shown below. If we do not configure and set targets to this file, then prometheus will only be monitoring itself. By setting windows exporter as the target as well, we will be able to monitor our system. We can also add other targets in this file to monitor them as well. 
8. Once windows exporter has been configured to the prometheus.yml file we will navigate to prometheus just how we did in step 9. For this presentation we will type “process\_cpu\_seconds\_total” to see the CPU usage for our system. We can also enter “prometheus\_http\_request\_total” to see how many http requests the system is getting and from where. Both screens will be shown below.
9. In the following screen we ran our previous installation of Wireshark together with Prometheus. We were able to see the time queries related to Prometheus and capture packet traffic with Wireshark on our ethernet connection.



## Recommendations

Prometheus offers a variety of options and tools to a user; however the usability of Prometheus is complex. To use this tool effectively it would be invaluable to install a graphical user interface, understand the programming/scripting, identify some customer support for the application, and review the best practices on the Prometheus website. The Prometheus website provides valuable resources. Below is more information on each of these recommendations.

* Graphical User interface (GUI):
  + There are a few options for a GUI with Prometheus. You can choose to design a template or install a tool called Grafana. This is encouraged because it takes the raw data from Prometheus and presents it in an easy to read dashboard. For more information about Grafana see the link below.
  + <https://prometheus.io/docs/visualization/grafana/>
* Training:
  + The toolkit Prometheus requires some configuration on the part of the user, within this includes establishing the metrics that outline how to identify unusual network activity. The Prometheus website recommends training courses with the Linux Foundation, PromLabs, and Robust Perceptions. Below is a link to the website's training recommendations.
  + <https://prometheus.io/support-training/>
* Commercial Support:
  + Due to the complex nature of this tool, we recommend identifying an organization that can support your company's use of the tool or identify a local technician to support operations of Prometheus. While this will add an additional cost to the tool, it would improve the functionality of the tool. Some of these organizations include: PromLabs, Container Solutions, NexClipper, and sysdig. Below is a link to Prometheus’s recommended companies to provide commercial support to their tool.
  + <https://prometheus.io/support-training/>
* Best Practices:
  + Additionally, Prometheus has identified some best practices when it comes to operating this toolkit. These have been identified and outlined to help the user effectively utilize their tools. Below is a link to the Best Practices section on Prometheus’s website.
  + <https://prometheus.io/docs/practices/naming/>

# Alternatives

Splunk’s Cloud Platform is a tool used to investigate, monitor and troubleshoot information technology environments to maintain uptime and monitor activity within your network. Splunk is a widely used tool within the information technology community and performs many different functions. There are different levels of Splunk that can be implemented. The base Splunk platform is free, however, to provide a comparable service to Prometheus, we would recommend the Splunk Platform, which is a usage based cost. This is based on cloud computing, memory, and I/O resources. For a smaller, primarily online organization, this would provide a scalable cost based on need. There are 3 additional specializations that can be included into Splunk, their IT, Security, and Observability functions. IT focuses on providing uptime and recovery assurance, which is an additional monthly cost of $40 per host. The Security function provides a Security Information and Event Management (SIEM) function to each device, the price point for this is a monthly per device charge of $5.75. The Observability function monitors network activities and integrates it into an easily understood format, this function starts at a monthly charge of $65 per host. Splunk is an industry standard tool used by many companies. The Ashburn’s Frog Emporium would benefit from the support and automation that Splunk provides. We would recommend implementing the Security Function due to the few devices on their network and it would provide effective detection and notification of incidents.

# Conclusion

Our security team was tasked with designing and implementing an integrated defense in depth structure to improve the information security of a small online and brick and mortar retailer. We installed, configured, and tested the Prometheus toolkit. It is a powerful network monitoring tool that allows for a variety of uses within the tool. With this customization comes some user difficulty. For a simpler network monitoring tool, we recommend Splunk. Splunk has some great features that would support Ashburn’s Frog Emporium’s goal of information security; however, Splunk would require a scalable monthly cost to use.

# Sources

“Prometheus.” *HGInsights*, Discover, 2021, https://discovery.hgdata.com/product/mandiant.

“Turn Data into Doing.” *Splunk*, Splunk, https://www.splunk.com/.

Hailey, Caleb. “An Introduction to Prometheus Monitoring (2021).” Sensu, Sensu, Inc., 1 June 2021, https://sensu.io/blog/introduction-to-prometheus-monitoring.

James Turnbull (12 June 2018). Monitoring with Prometheus. Turnbull Press. ISBN 978-0-9888202-8-9.

Prometheus. “Overview: Prometheus.” *Prometheus*, https://prometheus.io/docs/introduction/overview/.