HoneyPot Lab Manual

By: Cole Monpas, Rebecca Sharp, Lyndsey Pettit, Justin Costello.

Honeypot Wiki: <https://hp-wiki.cyberrangepoulsbo.com/>

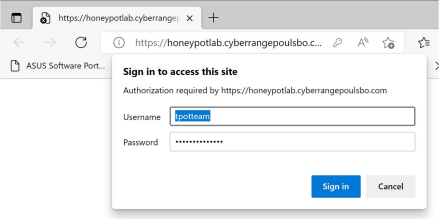
Getting Started

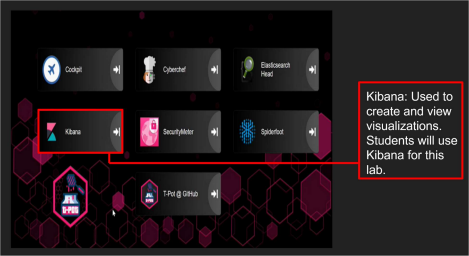
To get started open a browser > type in:

https//honeypotlab.cyberrangepoulsbo.com/

Username: tpotteam

Password: Pr0j3ct!W!n722

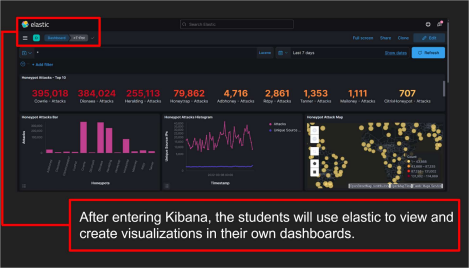
This will take you to the T-pot landing page > click on “Kibana”



A screenshot of a computer

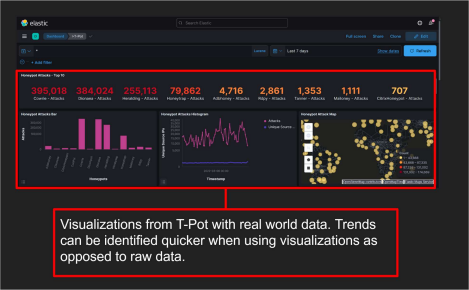
AI-generated content may be incorrect.

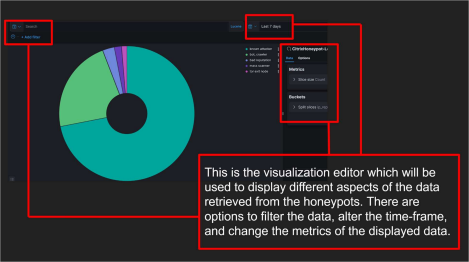
We need Cockpit for container and monitoring, elasticsearch for actual storage, Kibana for virtualization.



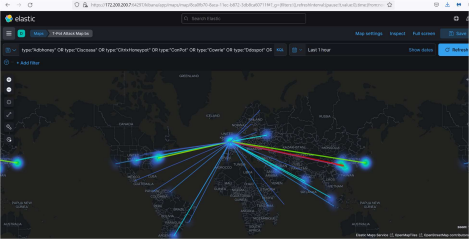
A screenshot of a computer

AI-generated content may be incorrect.





T-Pot attack map in elastic



NOTE: Make sure to pay attention to and follow along with the highlighted areas that tell you what activity you will be performing and what questions you must answer on the accompanied document.

Understanding Kibana Visualizations

When it comes to searching and viewing your Elasticsearch data, Kibana is your go-to tool. Security event analysis is one of the many uses for Kibana's visualization features. The following are the primary components that can be used for security analysis:

1. Discover is an event log search function that returns all logs matching a query [1].

2. Dashboards are visual representations that show the events in a visually rich context [1].

3. SIEM is the component you'll find specialized visualizations and queries for security analytics. Analysts can create a narrative utilizing the data in the SIEM component and a timeline tool [1].

4. The data from Elasticsearch can be used to train machine learning algorithms, which can then be applied to the data. Data anomalies can be detected using security-specific algorithms [1]. To learn more refer to this link: data anomalies

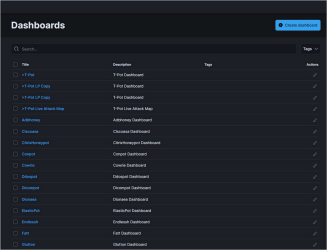
5. The graph component can be used to create graph relationships between objects contained within the same index [1].

6. In the Elastic stack, the Watcher component manages alerts. These alerts can be defined based on Elasticsearch queries on datasets [1].

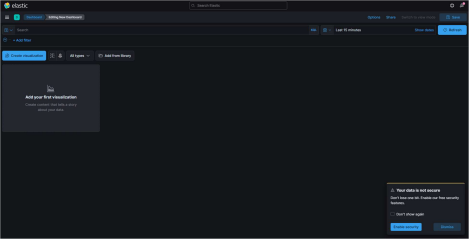
Great site to learn more: MITRE

The easiest way to get started with creating visualizations is to use Kibana Lens. Create Lens visualizations through basic drag-and-drop actions.

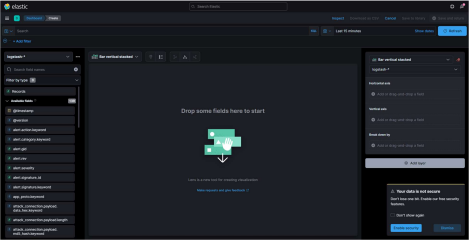
To start visualizing your data, begin by creating a new dashboard. Open Kibana by clicking the Kibana icon. This brings you to an overview with any existing dashboards

When you open Kibana you’ll be presented with the following page: 

Click Create dashboard in the top right corner to create a new dashboard. This brings you to an empty dashboard, to which you can add visualizations.

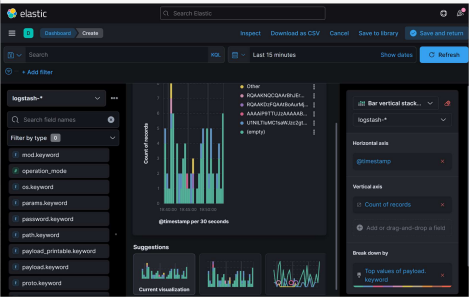


Click Create visualization to create a new visualization.



This launches the Lens drag-and-drop editor, which is divided into four sections. You can create queries and filters at the top. You can also specify the time period that interests you. On the left side, you can choose which indices to use. Below that is a list of fields available in the documents in the selected indices. When you click on a field, you can quickly get information about the data in that field, such as the most common values.

The visualization area is located in the center and is where your visualization will be displayed. Simply drag and drop a field into that area to begin creating a visualization. Lens can be seen attempting to guess how you want this field to be visualized.



If you want to visualize the data in a different way, you can try clicking on the suggestions that appear below the visualization area; however, you are not limited to these suggestions.

A dropdown menu with additional visualization options can be found just above the visualization area. The visualization can be customized on the right side. You can change the interval of the date histogram, for example, by clicking on timestamp.

Click on the field name under the vertical axis to visualize a metric other than the median. You can also change the color of the chart here. When you're satisfied with your visualization, save it and add it to the dashboard by clicking the save and return button in the top right corner. You can now resize and position this visualization anywhere on your dashboard.

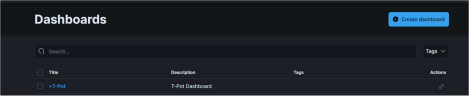
Click Create visualization again if you want to add another panel to your dashboard. You can also copy an existing visualization by selecting the Clone panel from the panel menu dropdown when you click on its panel menu dropdown.

Then you have the option of customizing the duplicated visualization in any way you want. When you're finished with your dashboard, save it by clicking the Save button in the toolbar. The Share option in the toolbar allows you to share your dashboard with

others. You can share a direct link to this dashboard with others. You can also generate a PDF report to send to people who do not have access to Kibana.

With our honeypot data, we can see that we have a pool of data about ongoing attacks, who are doing the attacks, and what ports they are targeting. This data can be used to produce intel reports knowing who the persistent attackers will also help you defend against their attacks. For additional ideas or help refer to this link, it will assist in exploring data and answering questions below:dashboard pannels

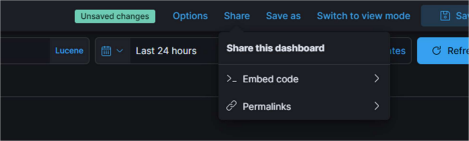
You will start by creating a simple chart or graph from a data chart. Do activity 1, from the question sheet.

Go back to Kibanas landing page and click on the Dashboard titled “T-Pot” Do question 1 from the question sheet.

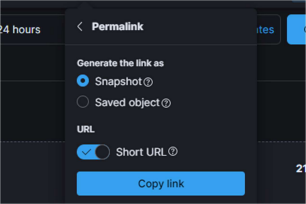


Now again go back to Kibanas main dashboard listings and click on the dashboard that was the most targeted honeypot. From here you can make a clone of the visualization and customize it to fit your needs for this assignment, or you can create your own visualization from what you learned above.

When you have finished with your customized visualization, click on Share in the top right corner.



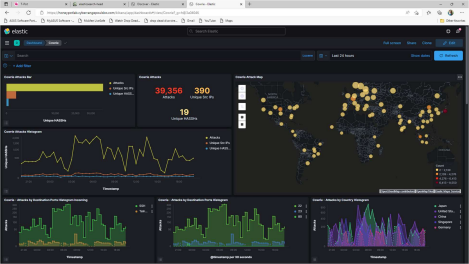
Now click on Permalinks > under URL slide the button that checks Short URL > click Copy link



Do activity 2 from the question sheet.

For some insight on how to examine data from point a to point b, refer to this link: data analysis

We want to investigate some of the malicious threat actors as well as the attacks that have occurred. Examine the data in your visualization to determine what stands out and why.



Do questions 2-4 from the question sheet.

Do activity 3.

Do question 5.

Investigate the IP that attacked the honeypot the most using sites such as https://www.abuseipdb.com/ or one similar.

Do activity 4.

Do question 6.

Let's look at what they do after they log in. We'll look at the command line output for this. When an attacker gains access to your system, it's critical to understand what they intend to do next. An attack isn't always launched by an unknown user with an unknown IP address. Most SIEMs allow you to set an alarm for any of the preceding actions. For example, if a user on your network loses their credentials and uses any of the following command sequences, you can flag it as suspicious activity and implement policies to block the account until the breach is validated.

Do question 7.

If the answer is no, find an IP address that gained access and input commands into the command line.

Do question 8.

Now lets do some scanner detection of high volume ports accessed. We can create detections for scanner-like behavior. These kinds of rules are simple to put in place. A search with aggregation based on unique elements, in this case destination port, can yield a list of source IPs attempting to connect to a large number of unique ports.

Outliers in these aggregations should be treated with suspicion. Take into account that public-facing servers are constantly being scanned by the internet. Internal servers, on the other hand, should not be subjected to this type of traffic at all.

Do questions 9-11.

ADDITIONAL HELP LINKS-

To understand what you are looking at and for:https://www.elastic.co/blog/understanding-and unlocking-security-data-sources-with-the-elastic-stack

Exploring fields (go to step 5): https://medium.com/@rpaezcysa/threat-analysis-t-pot-multi platform-honeypot-aws-ec2-cowrie-3be68c1193da

Using Elk as a honeypot dashboard:https://www.vanimpe.eu/2014/12/13/using-elk-dashboard honeypots/

https://www.elastic.co/guide/en/machine-learning/current/ml-configuring-categories.html patterns: https://phoenixnap.com/kb/kibana-tutorial

Sources:

[1] Mancini, Marco. “Security Analytics with Elastic.” Openaccess.Uoc.Edu, Dec. 2019, http://openaccess.uoc.edu/webapps/o2/bitstream/10609/113266/6/mmanciniTFM1219m emory.pdf.