Cyber Threat Hunting Lab

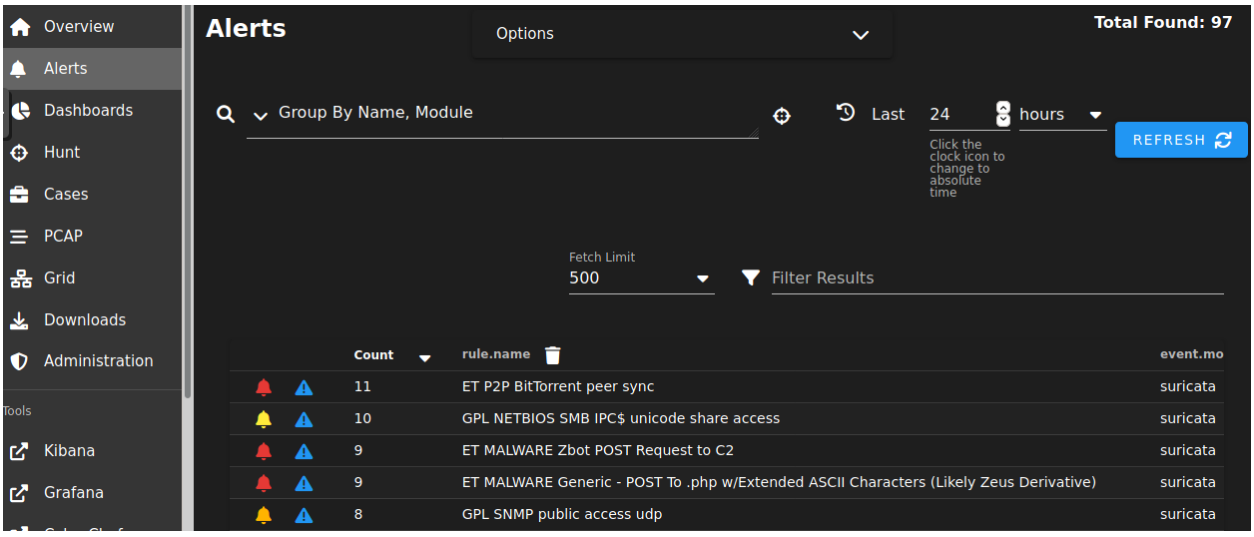
Objectives: Students completing this lab will be able to use and understand a Network Security Monitor (NSM) as part of a Security Information Event Monitoring system (SIEM). A dashboard will demonstrate alerts by time and severity; learners will be able to identify threats and categorize them, followed by cyber threat hunting based on the detected information.

Environment: You will access the NSM using your Kali (external) VM. Do not use Kali-Internal, as it will not properly resolve the DNS shortcut that we have created. All interactions will take place in a browser.

Accessing the NSM:

1. Log in to Proxmox with your user credentials. For CSP students, your coordinator will have sent these credentials to you. Be sure to use the PVE Authentication realm when you log in.
2. Open your Kali (external) VM - not your Kali Internal VM.
3. Open a web browser in Kali. Firefox or Chrome are acceptable. Click the start icon in the top left, select Favorites, and Web Browser.
4. In the URL bar, put: http://csp-nsm/
5. You will likely be prompted that the security certificate is not valid. Simply click “Advanced” and tell it to accept anyway.
6. Log in with username: csp@louisville.edu (not a valid e-mail address) and password: netsec2023!
7. Click “Alerts” on the menu to the left.

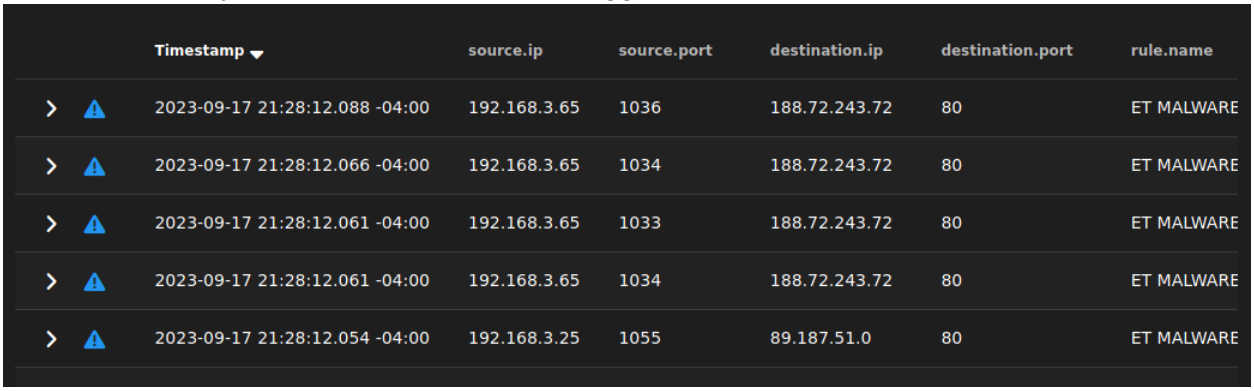
You will see a dashboard of alerts, by severity and with information. It should look like the image below:



Important: Do not click on the bell icon on an alert - the NSM is a shared resource; clicking the bell will acknowledge and delete the notification for others. If you check the alert console and do not see any alerts, please wait 12-24 hours and a new batch will appear.

Steps to Assess a Threat:

1. Click on the text of an alert with a red severity category, such as ET MALWARE
2. In the pop-up menu, go to “Hunt”
3. Scroll down and you should see entries that triggered the ruleset:



Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name
2023-09-17 21:28:12.088 -04:00	192.168.3.65	1036	188.72.243.72	80	ET MALWARE
2023-09-17 21:28:12.066 -04:00	192.168.3.65	1034	188.72.243.72	80	ET MALWARE
2023-09-17 21:28:12.061 -04:00	192.168.3.65	1033	188.72.243.72	80	ET MALWARE
2023-09-17 21:28:12.061 -04:00	192.168.3.65	1034	188.72.243.72	80	ET MALWARE
2023-09-17 21:28:12.054 -04:00	192.168.3.25	1055	89.187.51.0	80	ET MALWARE

4. Click the arrow on the left of an entry to expand the contents
5. Research the rule itself and see what has triggered it
6. Identify the geolocation of the IP address that is sending the offending traffic
7. Can you find any more information about the source of the traffic through searches?

Additional Discussion Questions:

1. Is it important to trim the rulesets that are triggering?
2. Can you find any rulesets that may be unnecessary based on the alerts you’ve seen?

Additional Information:

The SIEM is much more powerful than this introduction can cover. An alert can be escalated to a case where additional data is aggregated. Entries can be added to a case as needed. Furthemore, Security Onion has the ability to save all captured packets that are detected by the NSM. This allows play-by-play analysis of the data. You can check this out in the PCAP section of the menu.