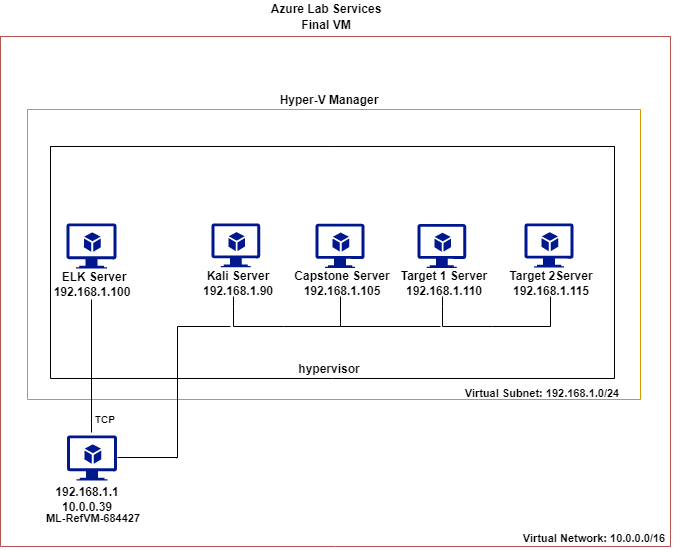
**Blue Team: Summary of Operations**

**Table of Contents**

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic & Behavior
* Suggestions for Going Further

**Network Topology**

**

The following machines were identified on the network:

* ML-RefVM-684427
  + **Operating System**: Windows
  + **Purpose**: Gateway Host for hypervisor
  + **IP Address**: 192.168.1.1
* Kali
  + **Operating System**: Linux
  + **Purpose**: Attacking Server
  + **IP Address**: 192.168.1.90
* Capstone
  + **Operating System**: Linux
  + **Purpose**: Server
  + **IP Address**: 192.168.1.105
* Target 1
  + **Operating System**: Linux
  + **Purpose**: Victim Server
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Linux
  + **Purpose**: Server
  + **IP Address**: 192.168.1.115

**Description of Targets**

The target of this attack was: Target 1 @ ip: 192.168.1.110

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

**Monitoring the Targets**

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

**CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* **Metric**: metricbeat
* **Threshold**: 0.5
* **Vulnerability Mitigated**: null\_pointer\_exception / DDOS
* **Reliability**: high reliability.

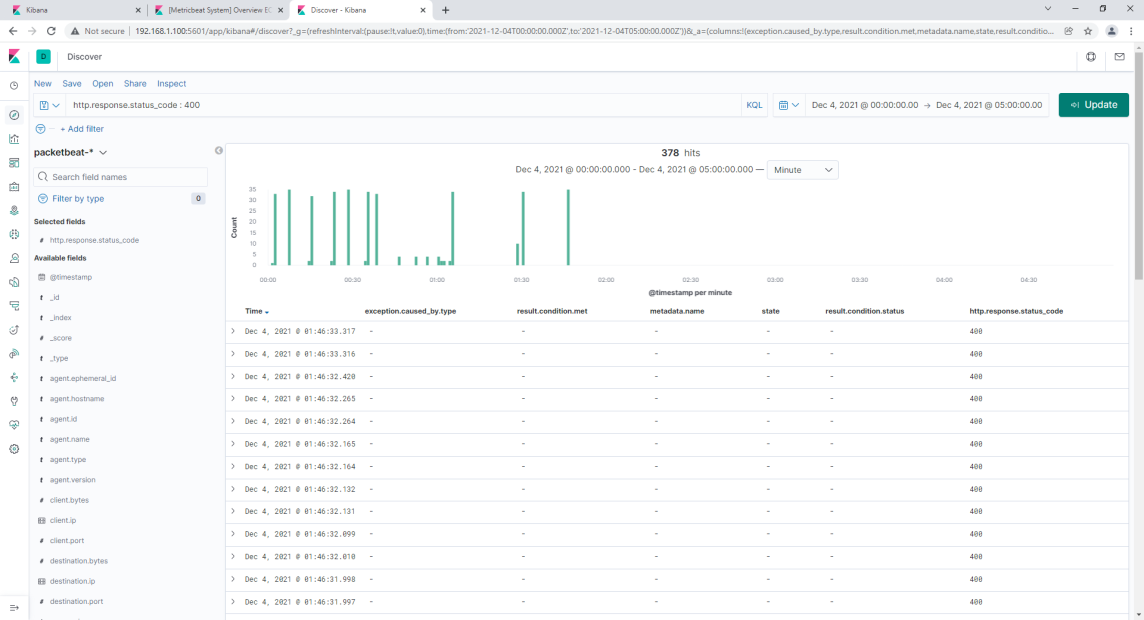
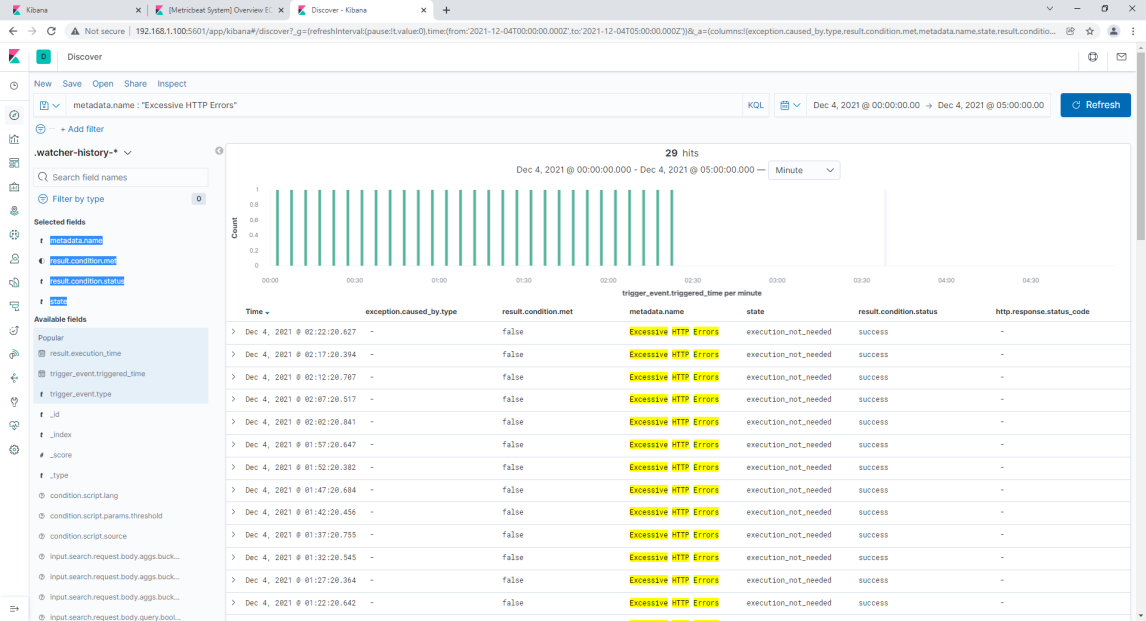
**HTTP Request Size Monitor**

HTTP Request Size Monitor is implemented as follows:

* **Metric**: packetbeat
* **Threshold**: 3500
* **Vulnerability Mitigated**: DDOS / Code Injection
* **Reliability**: low – The average packet size is approximately 237 to 338 bytes – so 3500 bytes is to far above the average to be responsive.

**Excessive HTTP Errors**

Excessive HTTP Errors is implemented as follows:

* **Metric**: packetbeat
* **Threshold**: 400
* **Vulnerability Mitigated**: Network Scan
* **Reliability**: low; alert generates lots of false positives/false negatives:
* 
* 

**Suggestions for Going Further (Optional)**

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

Overall Network Security should begin with:

* System updates and security patches
* Password strengthening to include uppercase, lowercase, numbers, special characters and increased length and complexity.
* Improved system and application control so that users have access to what is needed only. Make sure system resources are not allowing access to application or data incorrectly
* Implement multi factor login, bot check, and or lockout standards for all login points
* Deploy firewall and antivirus software
* **null\_pointer\_exception / DDOS**
* **Patch**:
  + Continue to use CPU Usage Monitor to Identify Normal and malicious DDOS attach traffic.
  + Identify critical systems and make sure that these are actively monitored for abnormal DDOS traffic
  + Configure and implement Intrusion Protection Systems or Intrusion Detection Systems to help monitor network traffic, alert, and respond.
  + Develop alert response that can route malicious DDOS traffic away from important servers (using DNS to reroute).
  + Once malicious IP addresses are identified employ snort rules to block traffic from that IP address.
  + **Why It Works**: Identifying DDOS attack patterns is a necessity. Once identified, processes must be put in place to reroute the attack and reset devices. Intrusion Protection Systems would work well to actively identify malicious traffic and enact your rules to mitigate attacks.
* **DDOS / Code Injectio**n
  + Modify HTTP Request Size Monitor threshold to recognize realistic code injection header size and abnormal packet size (closer to average of 237 – 338 bytes)
  + Elevate DB’s to require additional login and user login access levels prior to excepting SQL request.
  + Make sure all user input fields automatically remove harmful input prior to sending the input. Place an interface between applications and server database requests that disallows the server to send response back to unauthorized fields requests and or invalid certificates.
  + Physically separate DB servers systems
  + Use direct IP addressing to and from known IP addresses and ports and move these known connections when attacks are identified
  + Configure and implement log alerts, Intrusion Protection Systems, and Intrusion Detection Systems to help monitor and respond to malicious network traffic
  + **Why It Works**: Adding additional layers of protection to corporate data is essential. Identifying when packets are abnormal, pause processing, analyze the packet. Investigating the contents of a packet to see why the packet is blotted can help stop code injection. Also, identifying when packets have no value allow us to omit those packets from using resources. In the case of the wordpress update attack identified in Kibana, multiple updates where initiated to process zero length update files, this caused errors flooding that chocked out system resources. Intrusion Protection Systems, Intrusion Detection System, and log monitoring and alerts should be used to mitigate this.
* **Network Scan**
  + Modify the Excessive HTTP Errors alert to accurately identify the appropriate threshold level for error counts to indicate when IP addresses and ports are being scanned – also, if these errors are being generated from request from a single IP address - that is also a indicator. Pentest to get more accurate scan levels and correct baselines.
  + Configure and implement Intrusion Protection Systems, Intrusion Detection Systems to look for enumeration of the corporations IP addresses from a single IP address, accompanied with error responses. Drop the connection and add snort rules to block offending IP address traffic.
  + **Why It Works**: Identify when corporate IP addresses are being scanned by non authorized IP addresses, drop the connection, then prevent that from reoccurring.