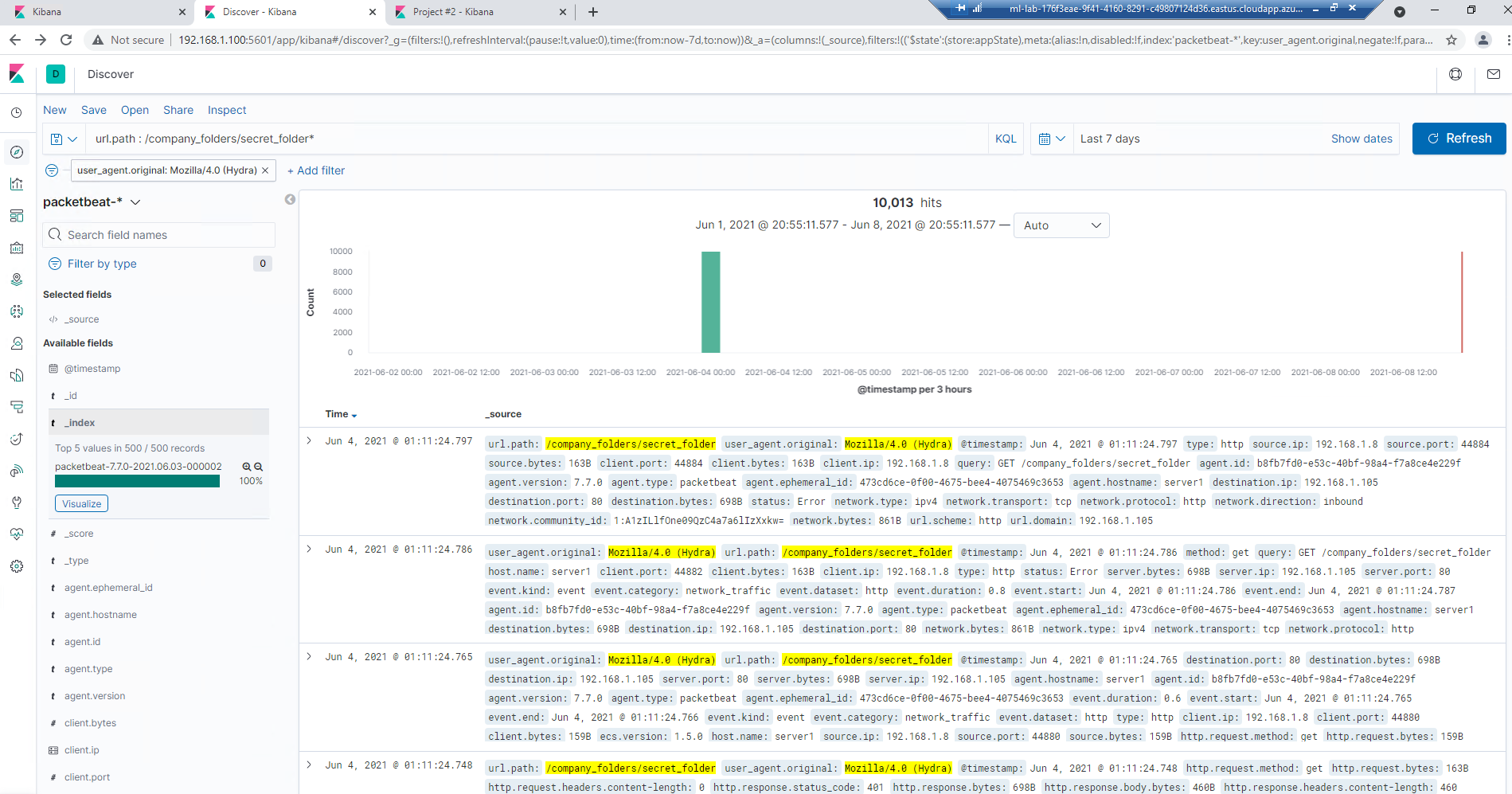
1. Identify the offensive traffic.  
   * Identify the traffic between your machine and the web machine:
     + When did the interaction occur? **2021-06-04 00:00**
     + What responses did the victim send back? **HTTP status codes for the top queries [Packetbeat] ECS**
     + What data is concerning from the Blue Team perspective? **Huge Spike in HTTP traffic in a condensed period of time: host traffic, error vs successful transaction**
2. Find the request for the hidden directory.  
   * In your attack, you found a secret folder. Let's look at that interaction between these two machines.
     + How many requests were made to this directory? At what time and from which IP address(es)? **10,019 hits; Jun 1, 2021 @ 20:43:19.785 - Jun 8, 2021 @ 20:43:19.785**
     + Which files were requested? What information did they contain? **url.path : "/webdav/passwd.dav" Ryan’s info**
     + What kind of alarm would you set to detect this behavior in the future?

**Set an alarm for that specific URL path to the secret folder**

* + - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

**Set up firewall rule to allow only authorized users from authorized IP addresses to access this folder**

1. Identify the brute force attack.  
   * After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:



* + - Can you identify packets specifically from Hydra?
    - How many requests were made in the brute-force attack?
    - How many requests had the attacker made before discovering the correct password in this one?
    - What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

1. Find the WebDav connection.  
   * Use your dashboard to answer the following questions:
     + How many requests were made to this directory?
     + Which file(s) were requested?
     + What kind of alarm would you set to detect such access in the future?
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.
2. Identify the reverse shell and meterpreter traffic.  
   * To finish off the attack, you uploaded a PHP reverse shell and started a meterpreter shell session. Answer the following questions:
     + Can you identify traffic from the meterpreter session?
     + What kinds of alarms would you set to detect this behavior in the future?
     + Identify at least one way to harden the vulnerable machine that would mitigate this attack.