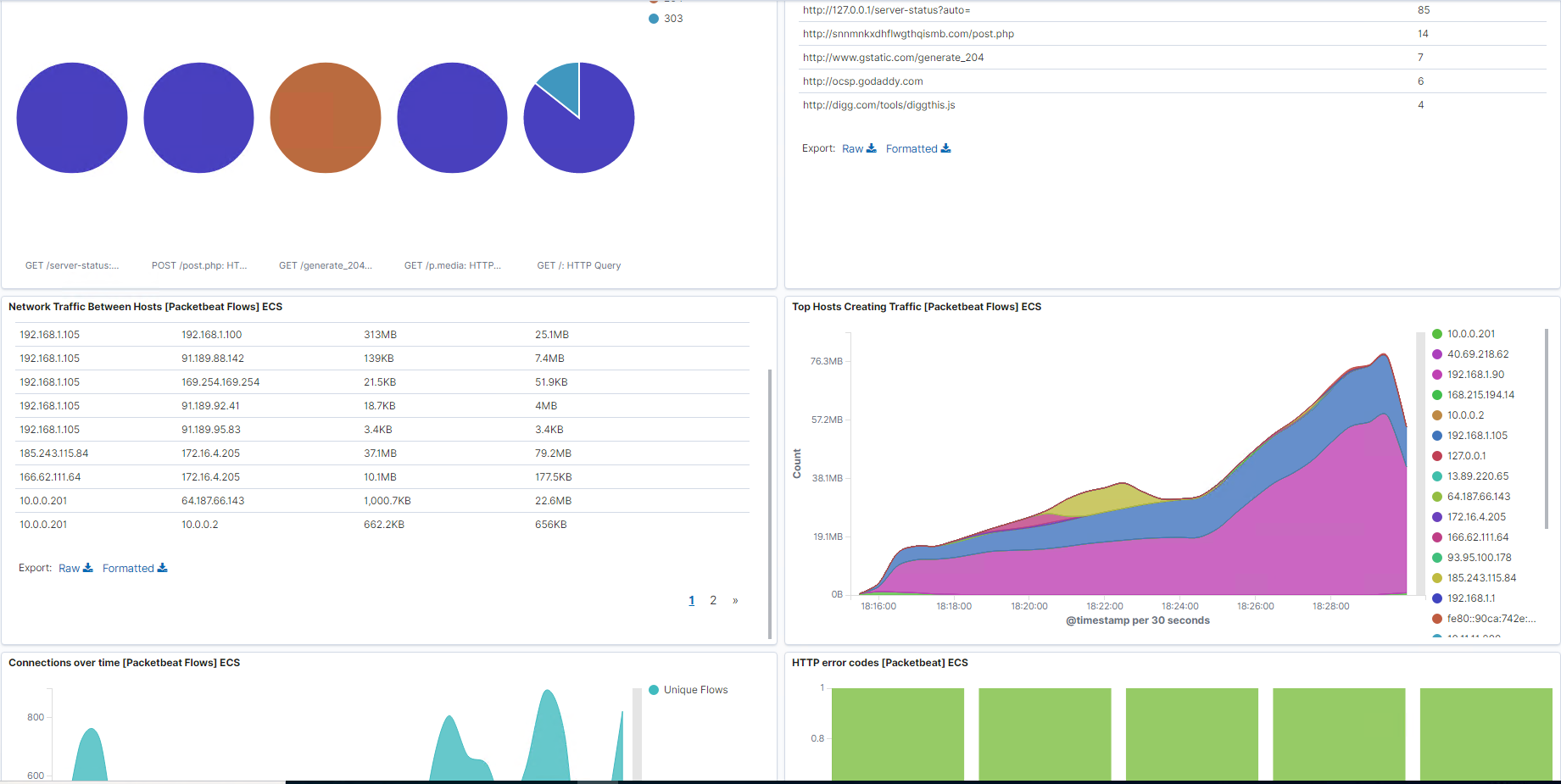
**Blue Team Exercise, Incident Analysis with Kibana**

The following data was loaded into Kibana for analysis of the Red Team attack:

1. Apache Logs
2. System Logs
3. Apache Metrics
4. System Metrics

A dashboard was created with the following eight reports:

* 1. HTTP status codes for the top queries [Packetbeat] ECS
  2. Top 10 HTTP requests [Packetbeat] ECS
  3. Network Traffic Between Hosts [Packetbeat Flows] ECS
  4. Top Hosts Creating Traffic [Packetbeat Flows] ECS
  5. Connections over time [Packetbeat Flows] ECS
  6. HTTP error codes [Packetbeat] ECS
  7. Errors vs successful transactions [Packetbeat] ECS



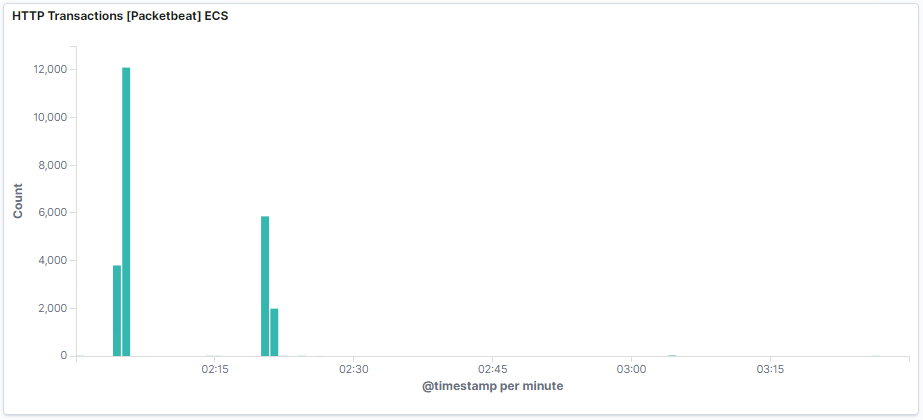
ATTACK ANALYSIS WITH KIBANA WORKFLOW

Identify the offensive traffic.

* Identify the traffic between your machine and the web machine:
  + When did the interaction occur?

**By querying traffic data source ip for the attacking and victim machines (192.168.1.90 and 192.168.1.105 respectively) traffic between the two machines took place between August 13, 06:20:00:000 MST and lasted through August 13, 08:26:06:796 MST (Figure 1).**

*Figure 1*



* + What responses did the victim send back?

**Initially, the victim sent back response code 200, ok, when navigating the victim’s site. When the secret\_folder was found which required a username and password and the brute force attack occurred, the victim responded with code 401, failed/unauthorized. After the brute force attack the response to the secret\_folder was code 200, ok.**

* + What data is concerning from the Blue Team perspective?

**Data that is concerning from the Blue Team perspective is the amount of traffic coming from the same ip address (the attacking machine 192.168.1.90, the fact that that ip address from an outside network is trying to access the secret folder, and how long the same ip address was accessing the site.**

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)?

**Four requests were made to this directory at the times in Figure 2:**

*Figure 2*



* + Which files were requested? What information did they contain?

**The secret\_folder directory was being requested which a file with directions to connect to the companies WebDAV server.**

* + What kind of alarm would you set to detect this behavior in the future?

**A good alarm to detect this type of behavior is to alarm when anyone is trying to access the secret\_folder and the http response code is 401.**

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

**One possible way to mitigate this attack is to not have the secret\_folder accessible via http connection.**

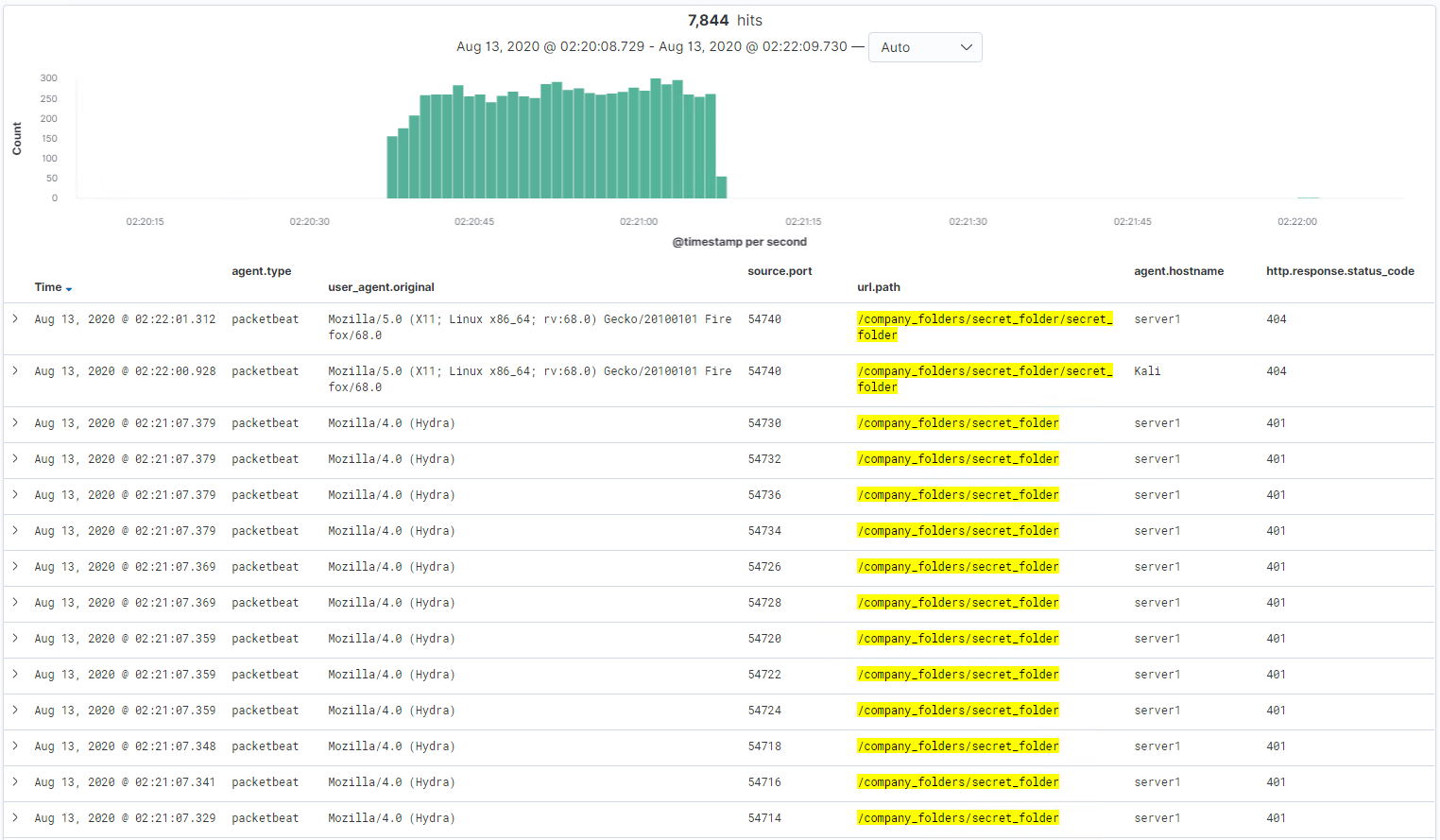
Identify the brute force attack.

* 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?

**Packets specifically from Hydra have a user\_agent.original field that says “Mozilla/ (Hydra)”. Also, there is a large amount of traffic with failed HTTP requests to the secret\_folder**

* + How many requests were made in the brute-force attack?

**7,844 requests were made in the brute-force attack.**



* + How many requests had the attacker made before discovering the correct password in this one?

**Same as above minus 1.**

* + What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?

**Alarms that go off when in a high number of attempts to login have been made from the same ip address and/or the user agent shows “Hydra” would detect of this type of behavior.**

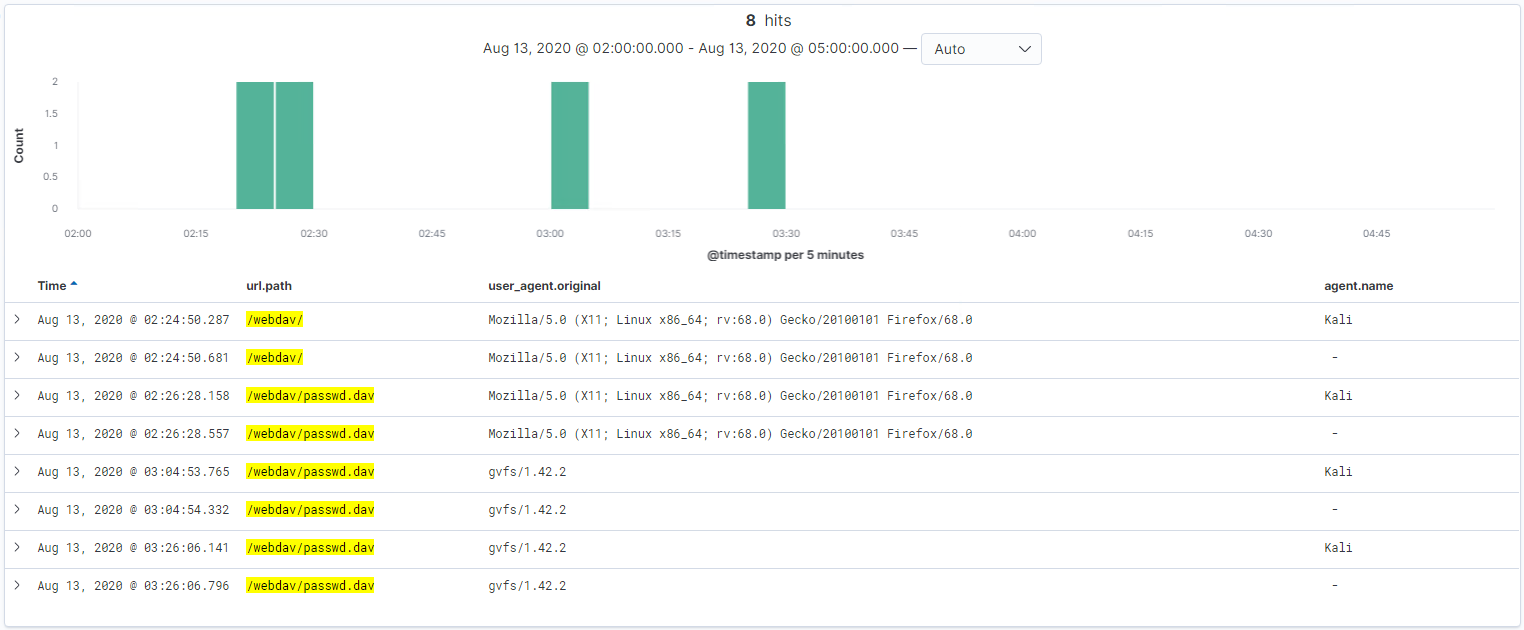
* + Identify at least one way to harden the vulnerable machine that would mitigate this attack.

**Setting limits on login attempts from a single source to that folder would harden the vulnerable machine to mitigate this type of attack.**

Find the WebDav connection.

* Use your dashboard to answer the following questions:
  + How many requests were made to this directory?

**8 requests were made to this directory.**



* + Which file(s) were requested?

**The password.dav file was being requested in the WebDAV server.**

* + What kind of alarm would you set to detect such access in the future?

**To detect such access to the WebDAV server I would set an alarm to alert when any ip address outside of the company network is trying to access this server.**

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

**To harden this vulnerable machine the directions to access the server should not be kept on a public site.**

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?

**Because I set up the meterpreter session port to be port 80 instead of 4444, the only way to see the meterpreter session is to look for network traffic from the attacking machine’s IP on port 80.**

* + 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.