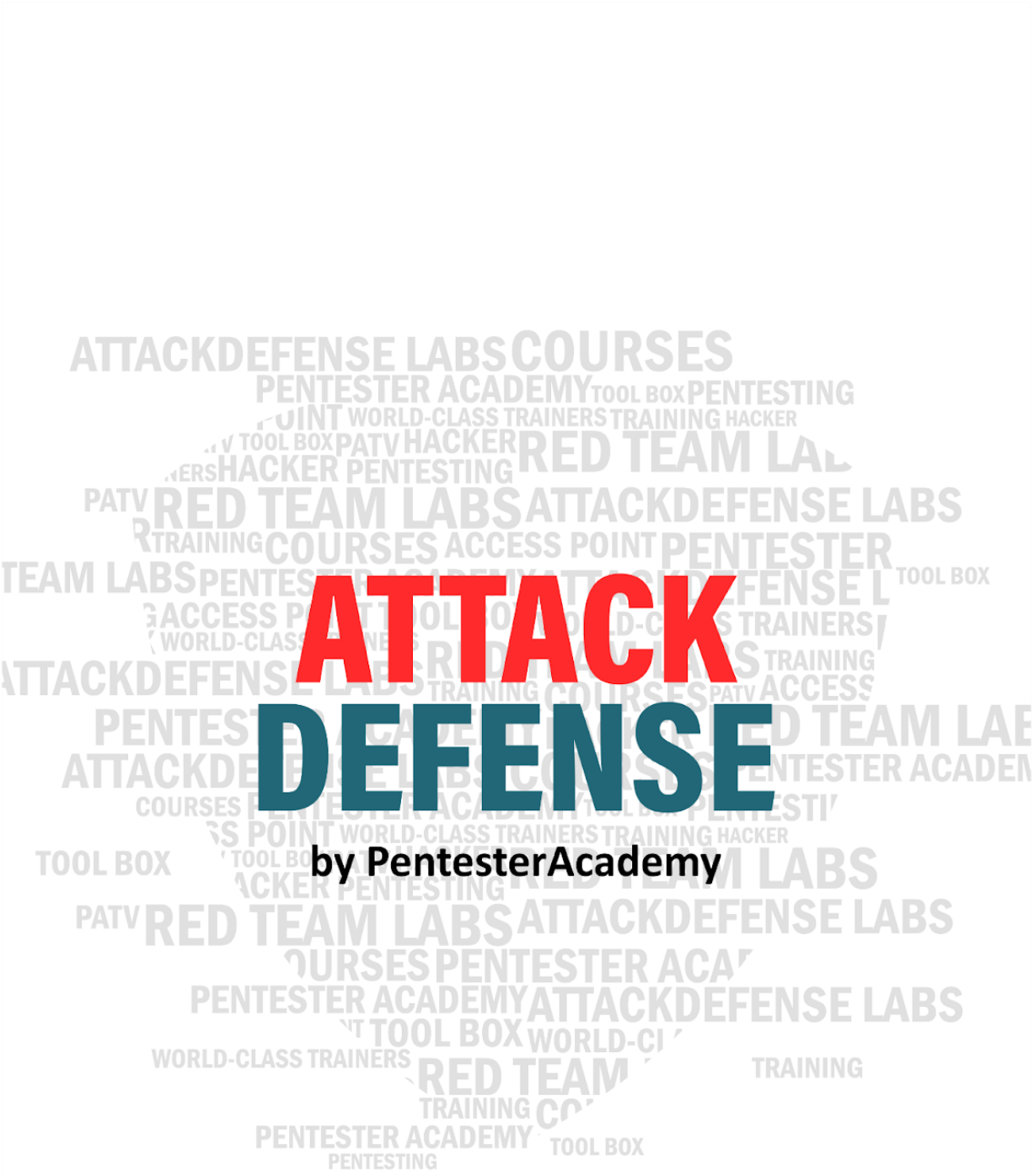
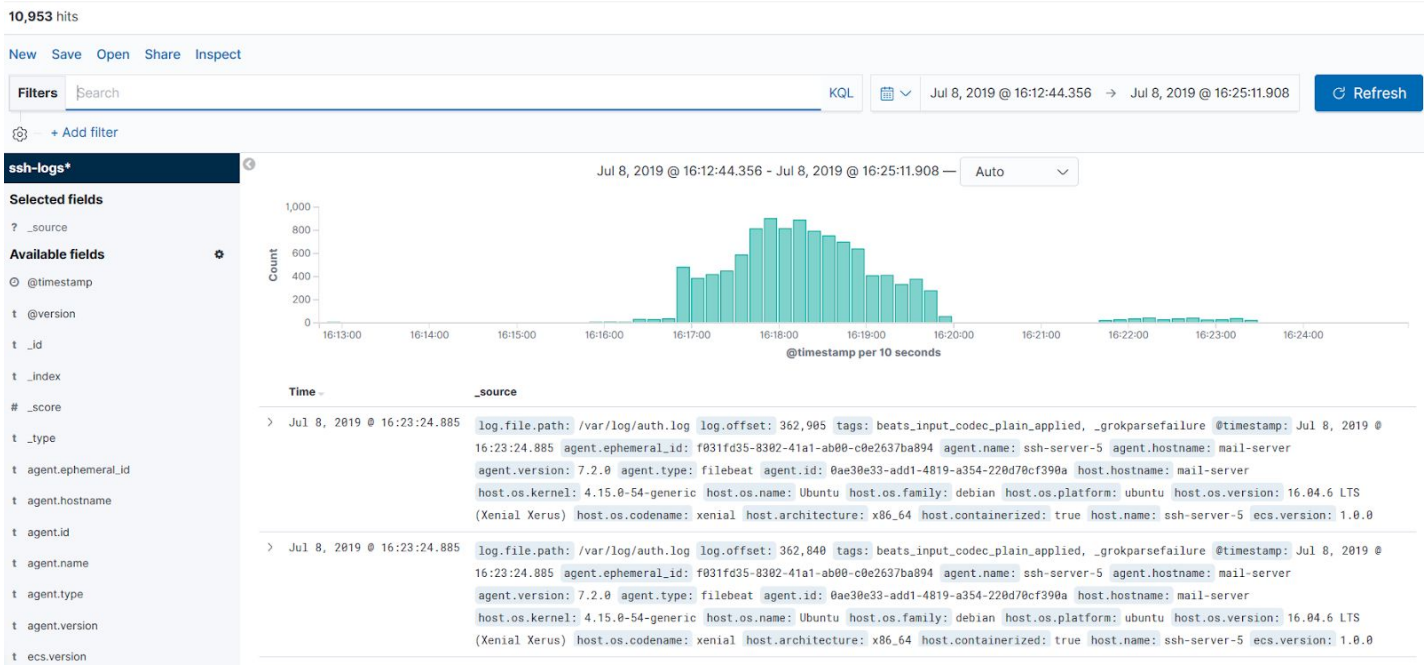

ATTACK
DEFENSE
by PentesterAcademy

Name	ELK: SSH Logs
URL	https://attackdefense.com/challengedetails?cid=1138
Type	Forensics : SSH Log Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Kibana and Elasticsearch setup is provided with SSH logs of multiple server machines. You have to analyze the logs using Kibana interface and answer the following question:

Kibana Dashboard



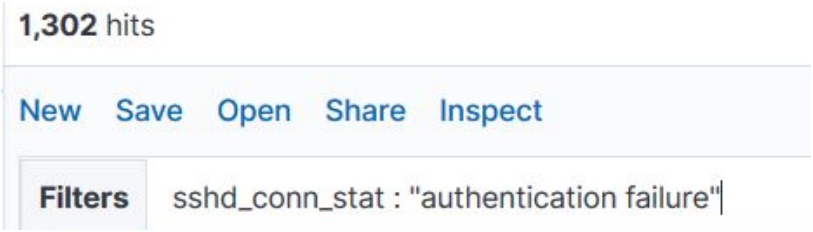
Q1. How many machines were attacking the SSH servers?

Answer: 3

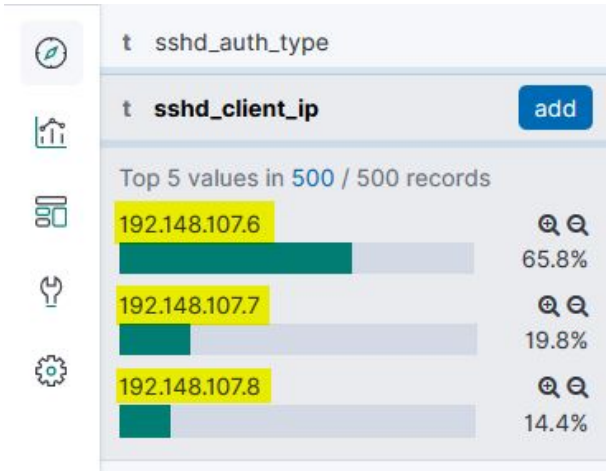
Solution:

Step 1: Apply the following filter to show all the logs related to ssh authentication failure.

Filter: sshd_conn_stat : "authentication failure"



Step 2: Check the 'sshd_client_ip' field in the “Available fields” list.



There were 3 clients with IP addresses 192.148.107.6, 192.148.107.7 and 192.148.107.8 involved in the attack on the SSH servers.

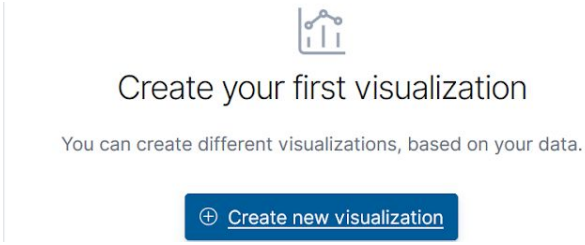
Q2. Which machine made the most SSH login attempts?

Answer: 192.148.107.6

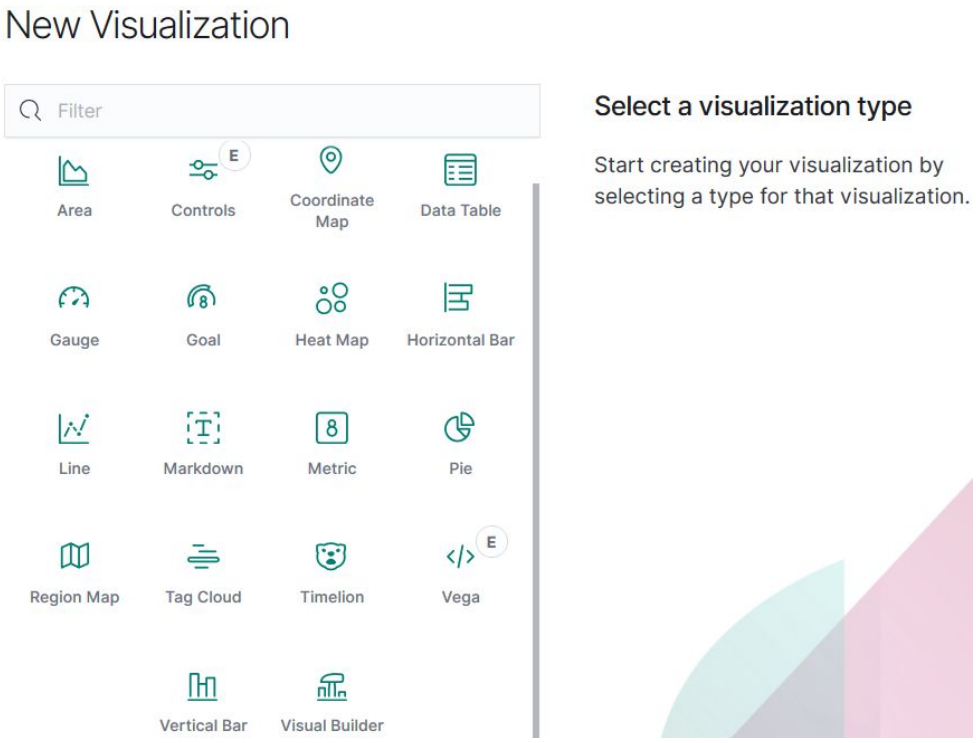
Solution:

Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.

Step 2: Click on 'Create new visualization'.

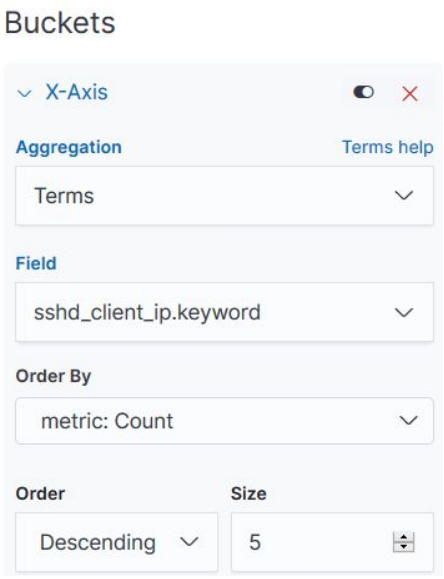


Step 3: Select 'Vertical Bar' Visualization.

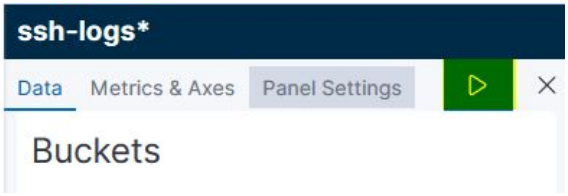


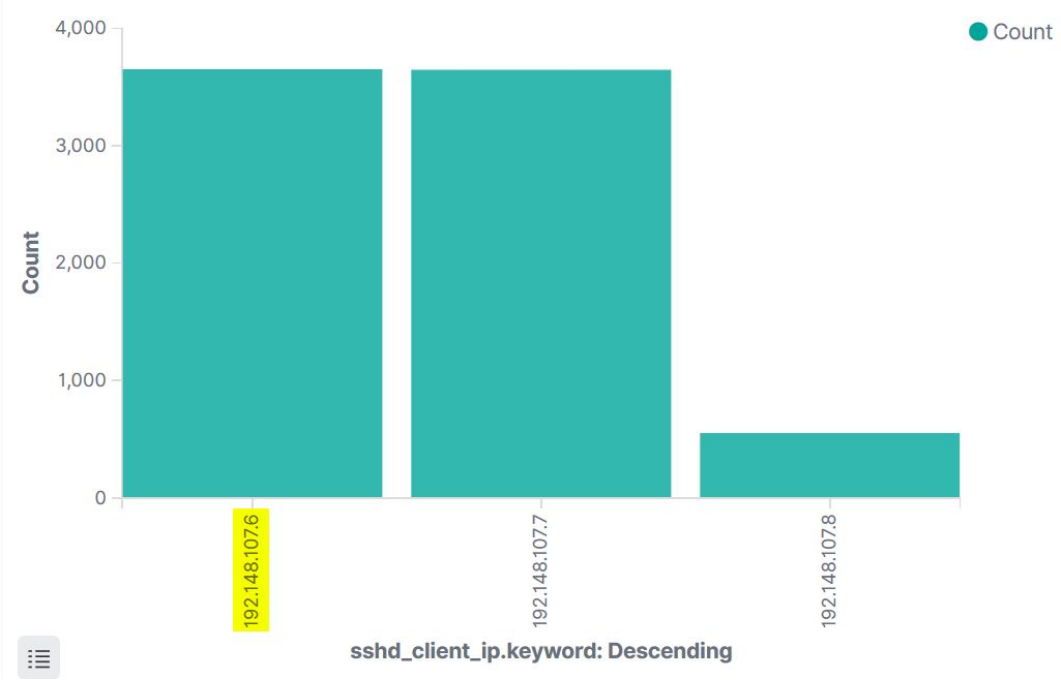
Step 4: Choose the ssh-log* index pattern as the source.

Step 5: Apply 'Terms' aggregation on 'ssh_client_ip.keyword' field.



Step 6: Press the 'Apply changes' button.





From the visualisation, it is evident that the client machine with IP address 192.148.107.6 made most login attempts.

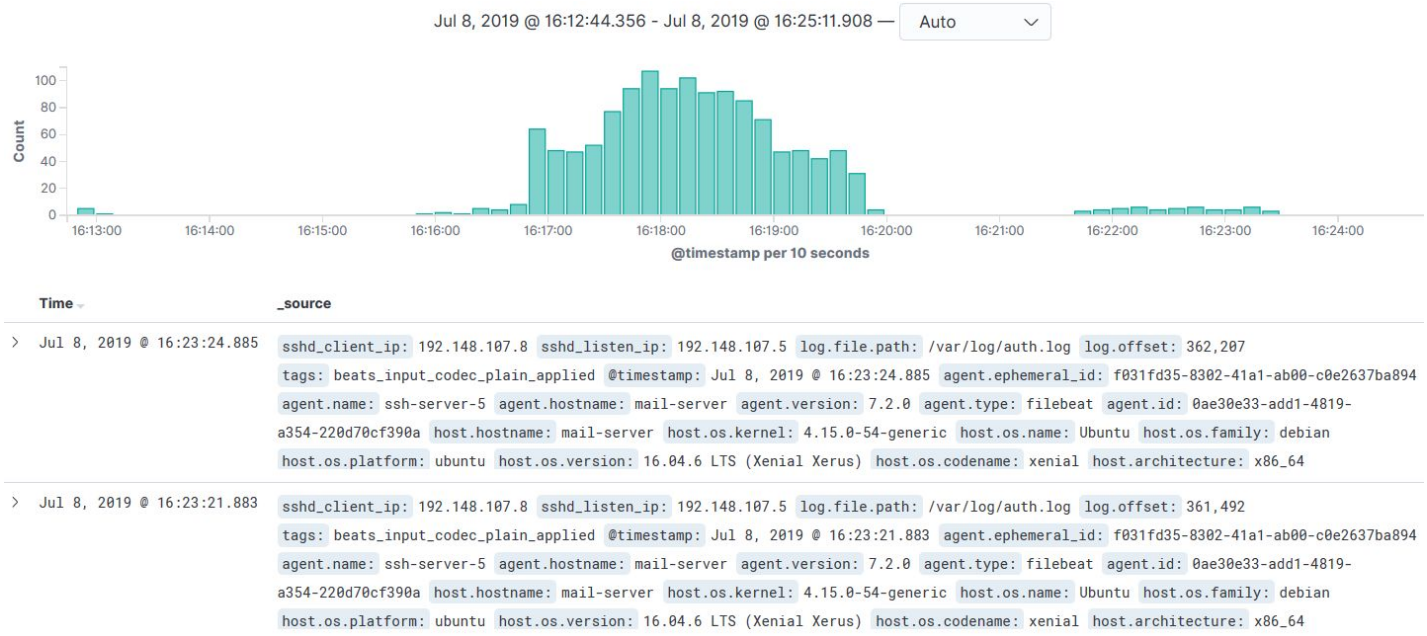
Q3. How many servers running SSH service were attacked?

Answer: 3

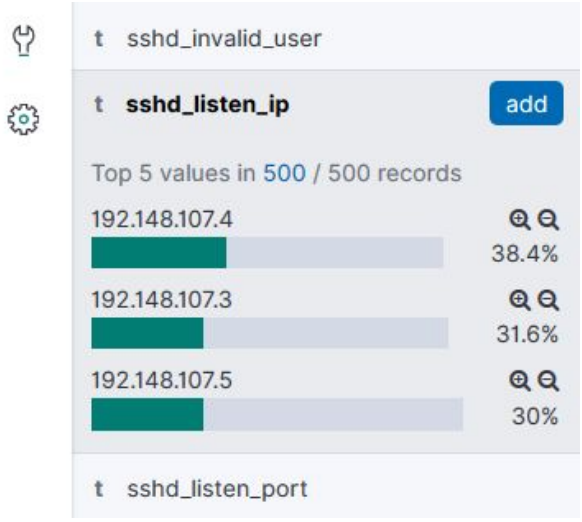
Solution:

Step 1: Apply the following filter to view all the logs which contain SSH server IP address.

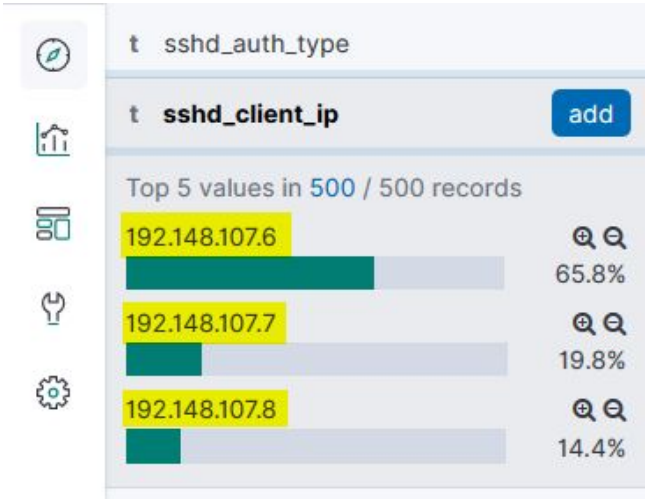
Filter: sshd_listen_ip : *



Step 2: In the “Available fields” list, check the 'sshd_listen_ip' field.



There were a total of 3 SSH servers. Now, check the 'sshd_client_ip' field in the “Available fields” list.



All these IP addresses are the same as the attacker IP addresses (found in question 1). hence, all 3 SSH servers were attacked.

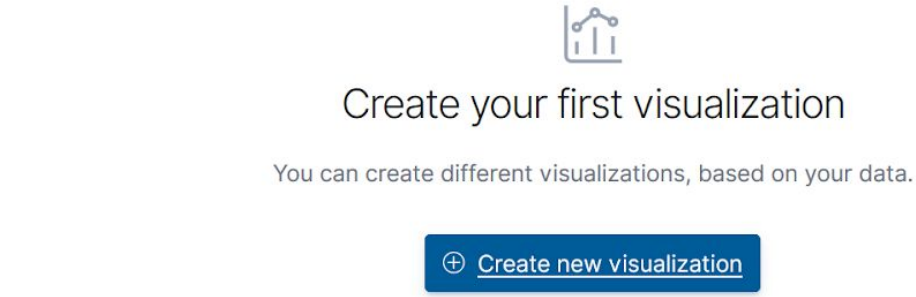
Q4. What is the IP address of the attacker machine that made the maximum login attempts on the most attacked SSH server?

Answer: 192.148.107.6

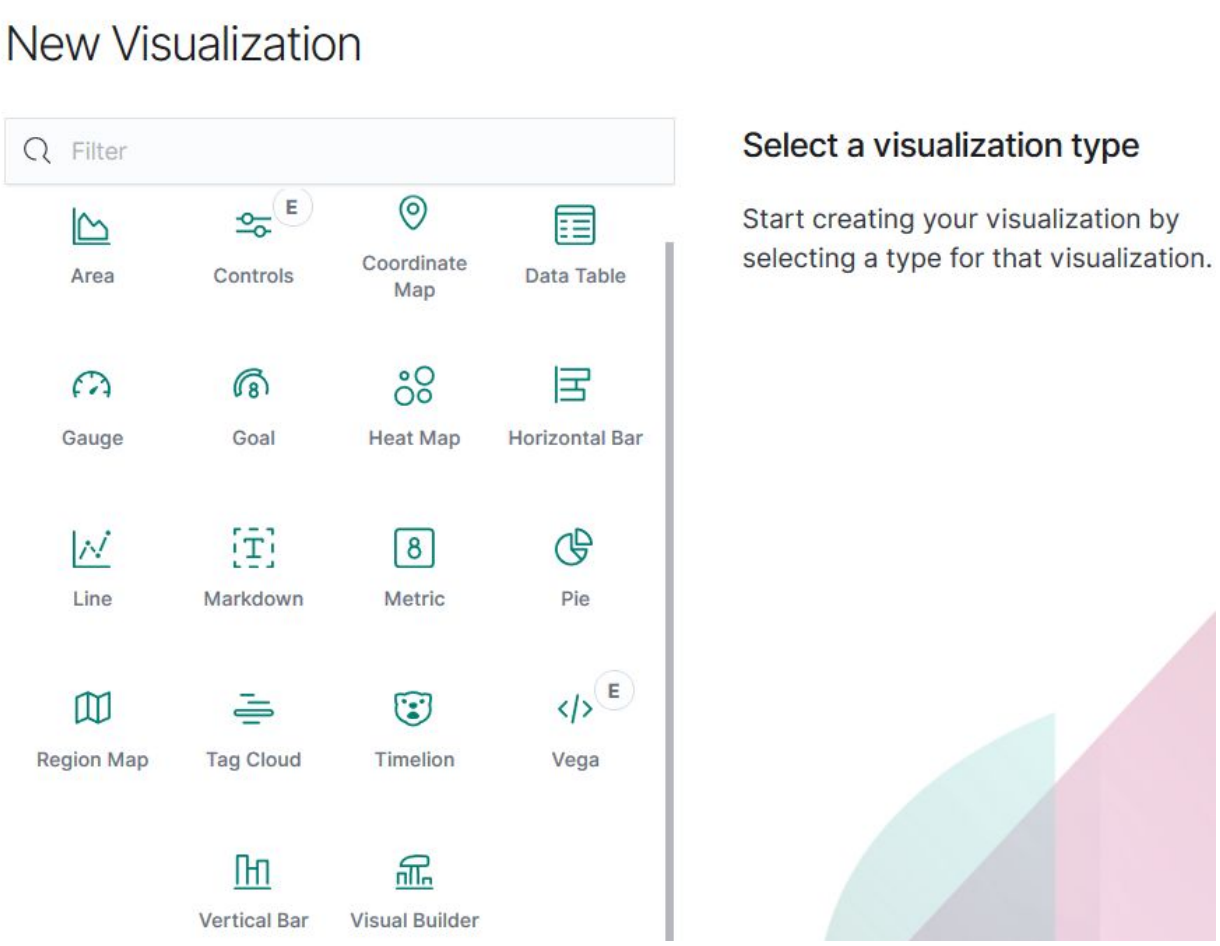
Solution:

Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.

Step 2: Click on 'Create new visualization'.



Step 3: Select 'Pie' Visualization.

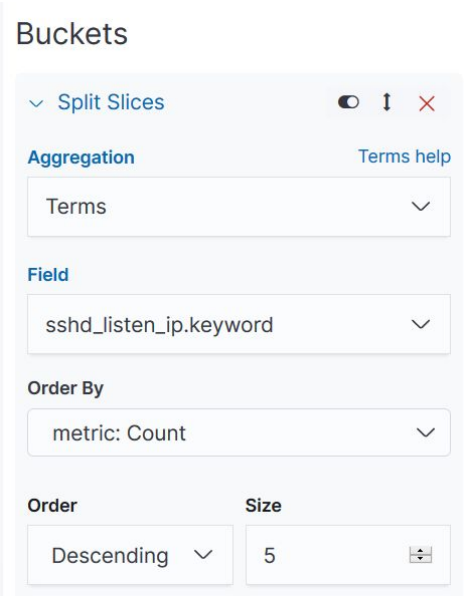


Step 4: Choose the ssh-log* index pattern as the source.

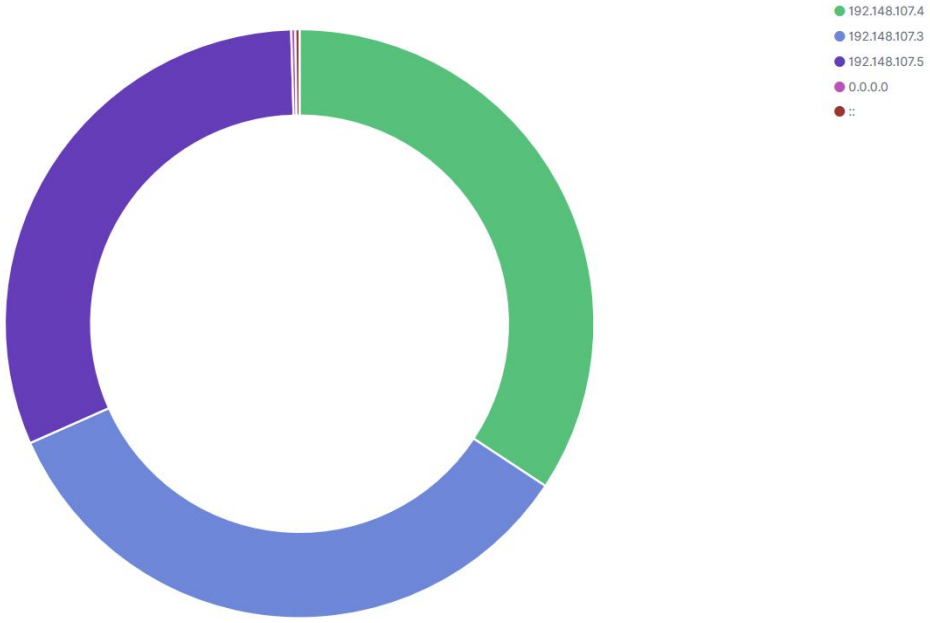
Step 5: Split the slices of the pie based on the SSH server count.

Select 'Split Slices'.

Apply 'Terms' aggregation on the field 'sshd_listen_ip.keyword', keeping other values as the default.



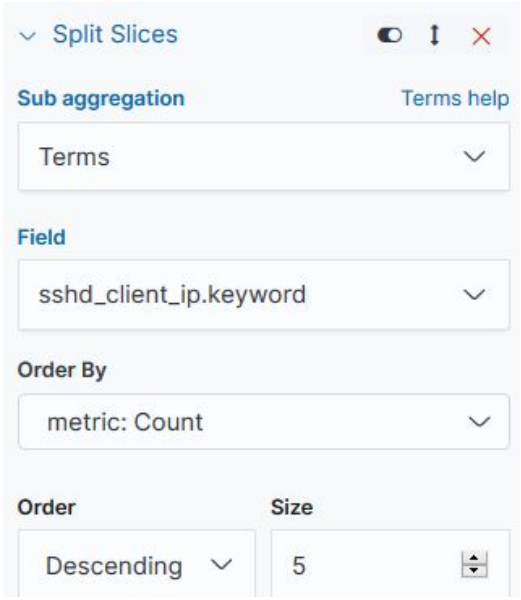
This will result in a pie chart representing the SSH servers in terms of attack share. Ignore the 0.0.0.0. and :: IP addresses as not valid IP addresses. These appear due to the initial SSH server start logs.

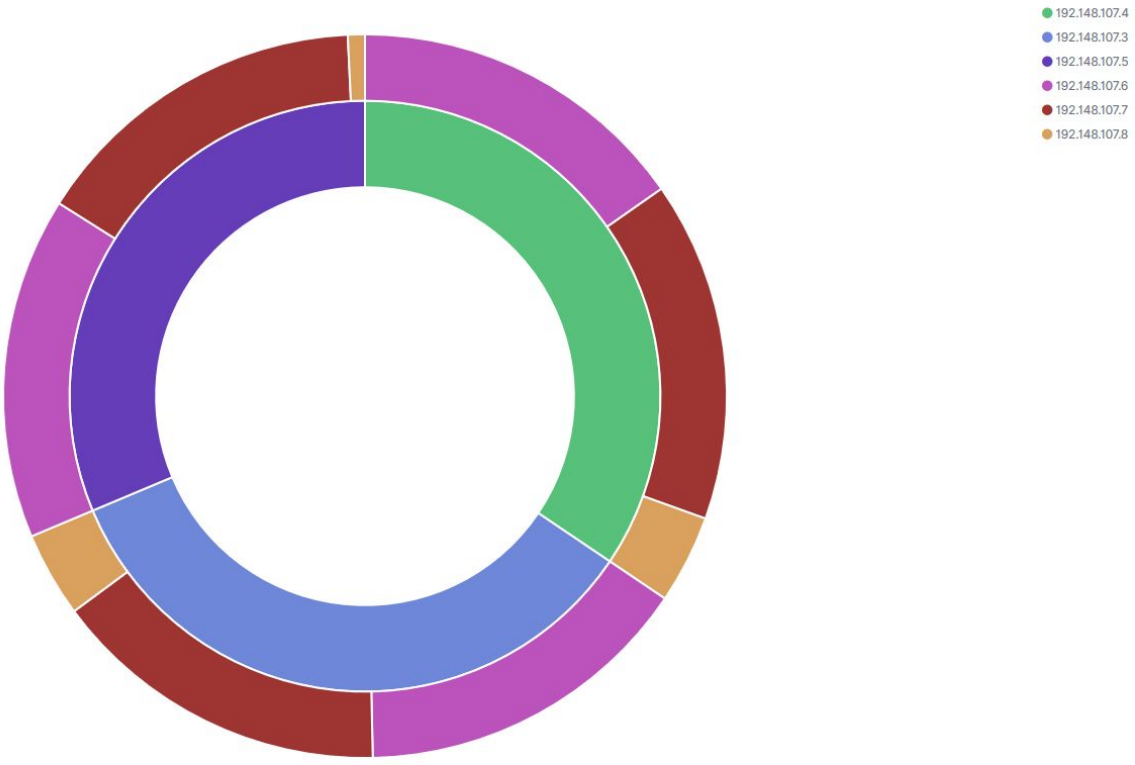


Step 6: Add a ‘sub-bucket’ to the above bucket (the pie visualization created in last step).

Select 'Split Slices'.

Step 7: Use 'Terms' sub-aggregation on 'sshd_client_ip.keyword' field.





From the level 1 pie (the inner pie), it is evident that the server with IP address 192.148.107.4 was attacked most.

The level 2 pie (the outer pie) reveals that the most active attacker trying to break into the server was one with the IP address 192.148.107.6.

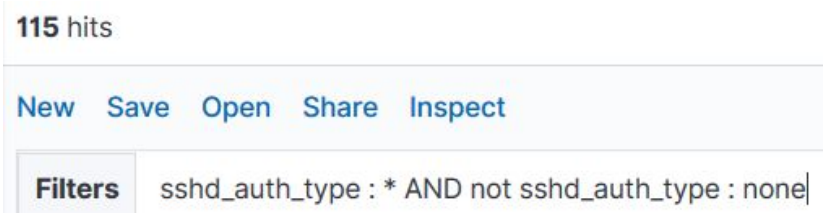
Q5. How many SSH authentication modes were used by the attacking machines to break into the servers?

Answer: 2

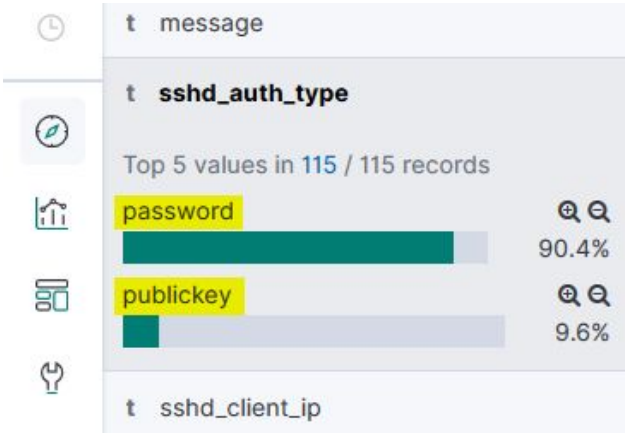
Solution:

Step 1: Apply the following filter to show all the logs where “sshd_auth_type” field exists and is not equal to “none”.

Filter: sshd_auth_type : * AND not sshd_auth_type : none



Step 2: Check the 'sshd_auth_type' field in the “Available fields” list.



Two authentication modes were used by the client machines i.e. public key and password authentication.

Q6. What was the IP address of the attacker machine which used public key authentication to break into the SSH servers?

Answer: 192.148.107.8

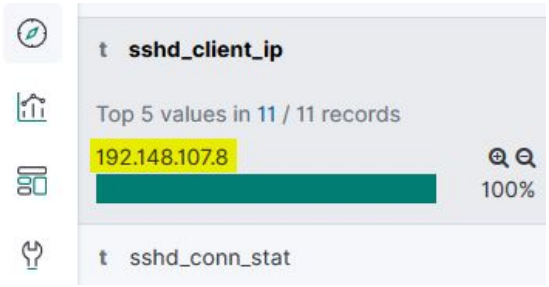
Solution:

Step 1: Apply the filter to show all the logs where the SSH authentication mode is publickey.

Filter: sshd_auth_type : "publickey"

Step 2: Open one of the matched documents and view its “message” field.

Alternatively, the 'sshd_client_ip' field in the “Available fields” list would also show the client IP address.



Hence, the client with IP address 192.148.107.8 used public key authentication to break into the SSH servers.

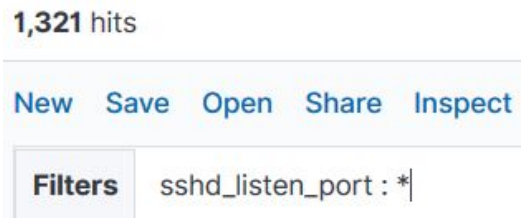
Q7. SSH service was running on which port on all the servers? Provide port number.

Answer: 3603

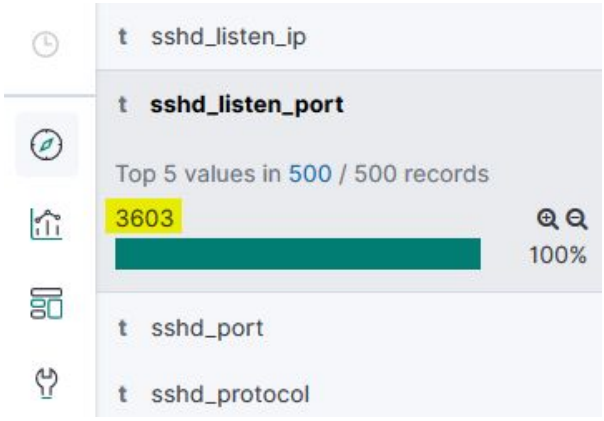
Solution:

Step 1: Apply the following filter to show all the logs where “sshd_listen_port” field exists.

Filter: sshd_listen_port : *



Step 2: Check the value of 'sshd_listen_port' in the “Available fields” list.



SSH was running on port 3603 on the servers.

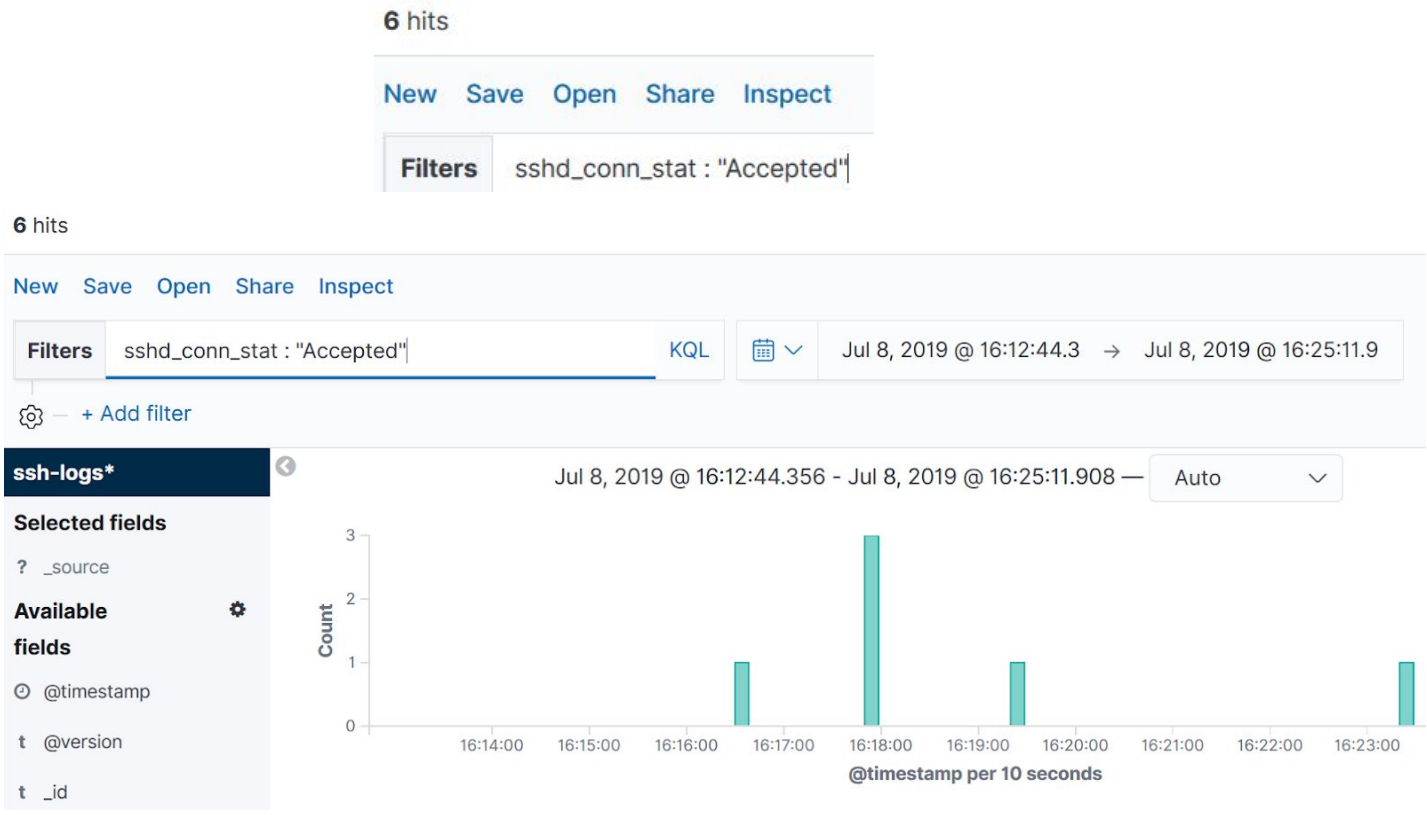
Q8. What is the name of the user account that got compromised on the SSH servers?

Answer: administrator

Solution:

Step 1: Apply the following filter to show all the logs where the SSH connection status is “Accepted”.

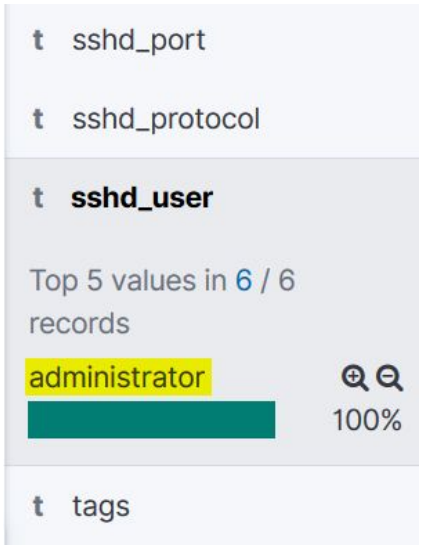
Filter: sshd_conn_stat : "Accepted"



Step 2: Open one of the matched documents. The 'message' field shows that the user 'administrator' got compromised.

t	message	Jul 8 16:23:24 ssh-server-5 sshd[916]: Accepted password for administrator from 192.148.107.8 port 57690 ssh2
t	sshd_auth_type	password
t	sshd_client_ip	192.148.107.8

Alternatively, check the 'sshd_user' field in the “Available fields” list.



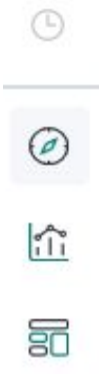
Thus, ‘administrator’ user account was compromised on the SSH servers.

Q9. At what time the maximum number of logs were pushed into elasticsearch? Provide the time in HH:MM:SS format.

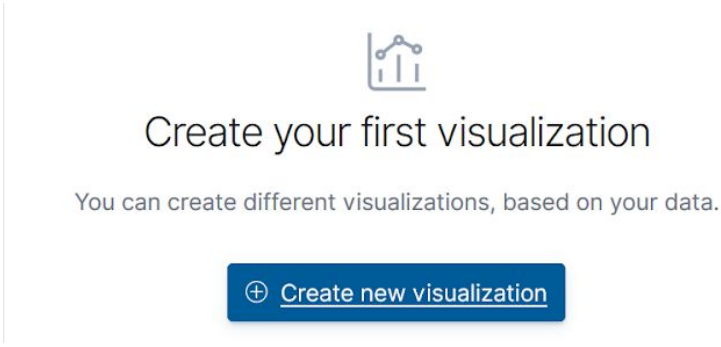
Answer: 16:17:58

Solution:

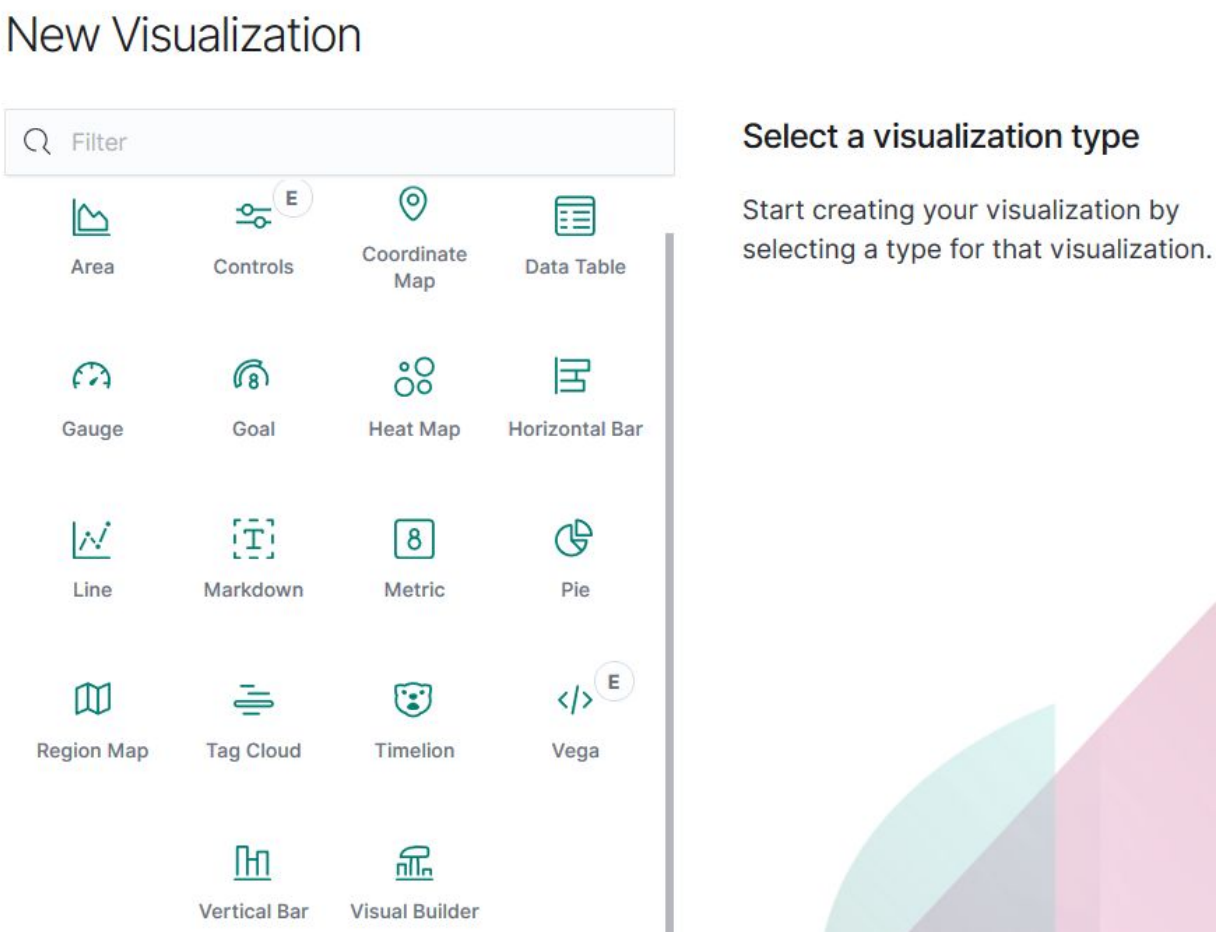
Step 1: Create a visualization to figure this out. Navigate to the 'Visualize' Section.

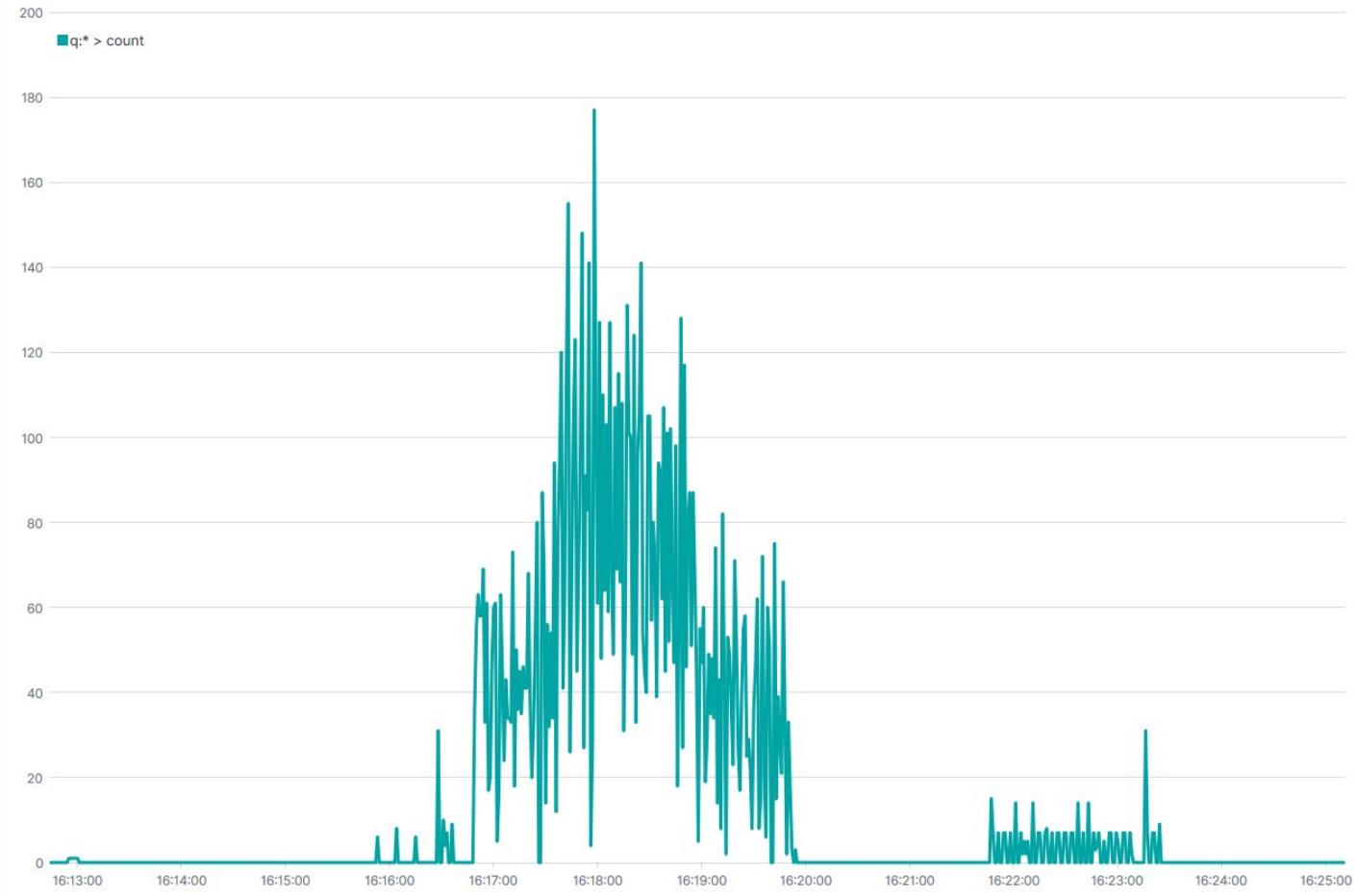


Step 2: Click on 'Create new visualization'.

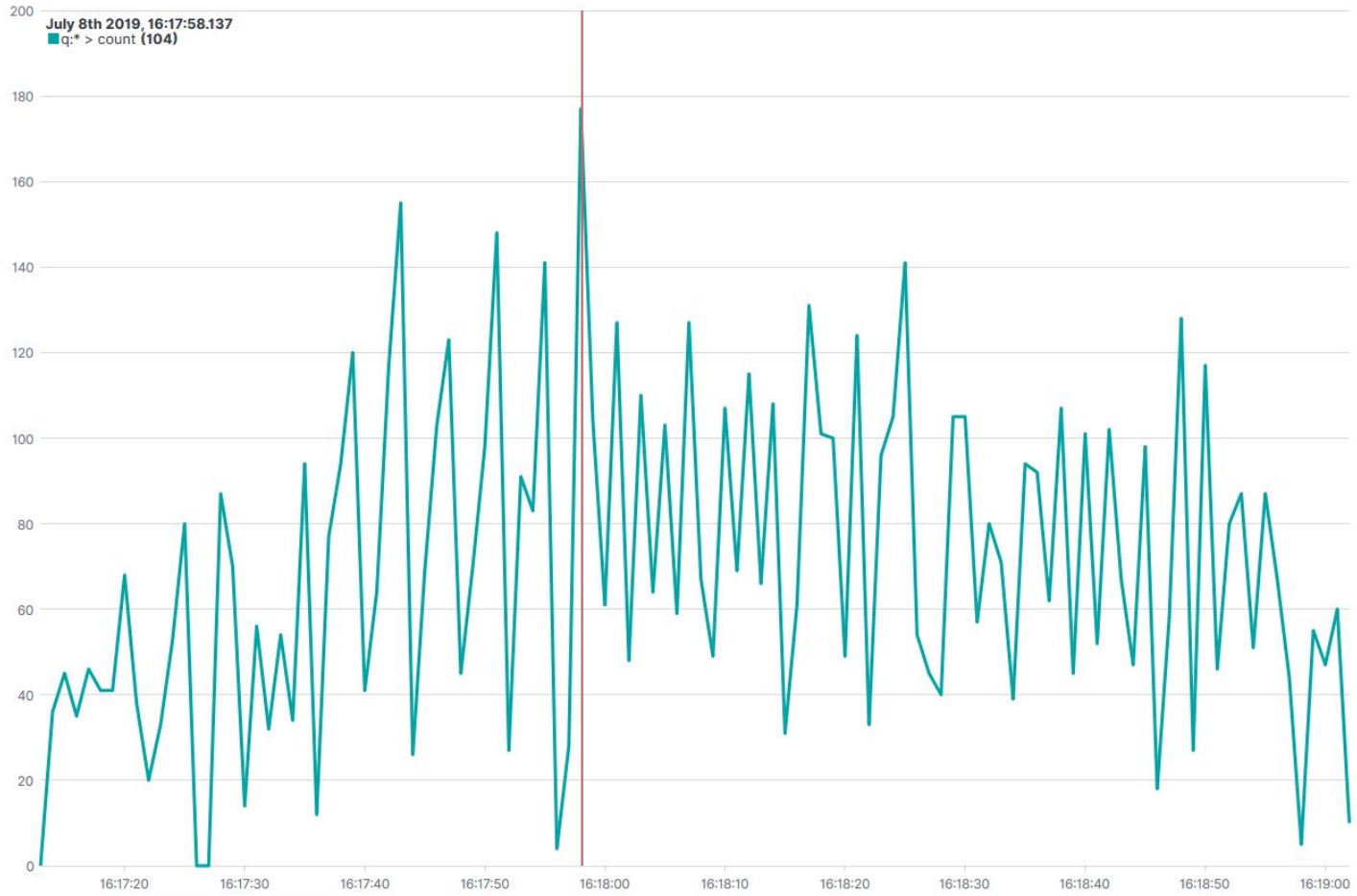


Step 3: Select 'Timelion' Visualization.





Step 4: Zoom into the peak region.



At 16:17:58 maximum number of logs were pushed into elasticsearch.

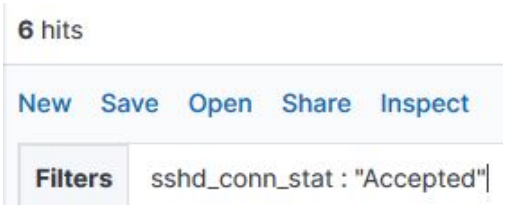
Q10. What is the IP address of the SSH server that got compromised first?

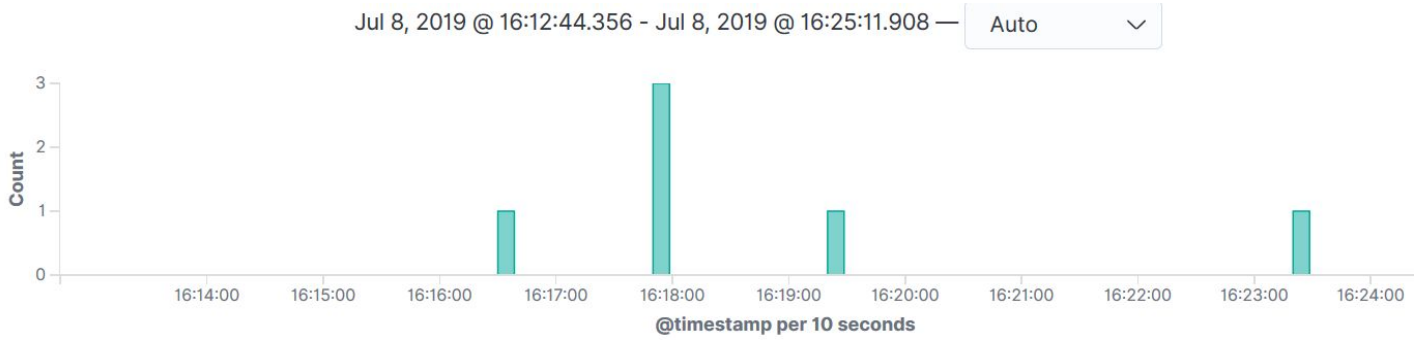
Answer: 192.148.107.3

Solution:

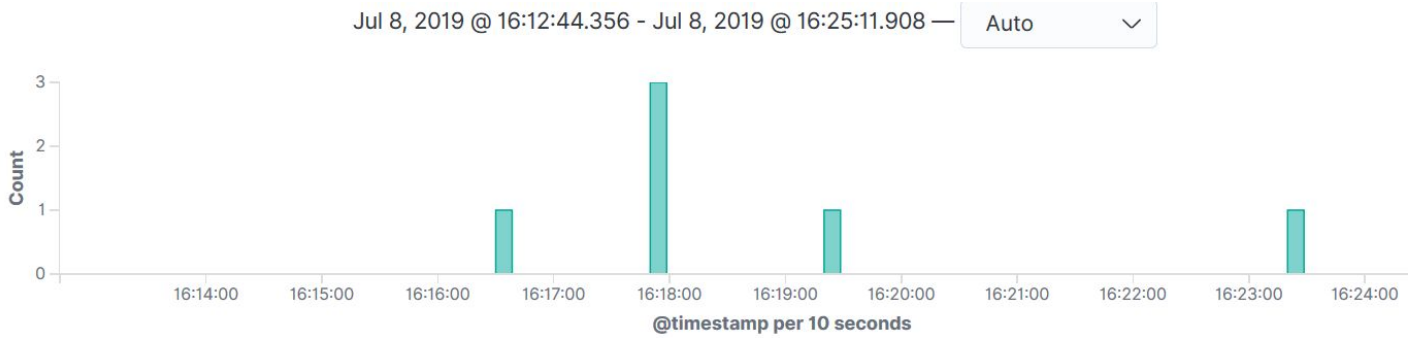
Step 1: Create a visualization to figure this out. Apply the following filter to show all the logs where the SSH connection status is “Accepted”.

Filter: sshd_conn_stat : "Accepted"





Step 2: The first bar indicates the first compromised SSH server.



This bar corresponds to the last document among the list, since the list has been sorted in descending order based on time. This document will be required to get the host.name

> Jul 8, 2019 @ 16:17:58.191 sshd_conn_stat: Accepted sshd_user: administrator tags: beats_input_codec_plain_applied sshd_protocol: ssh2 @timestamp: Jul 8, 2019 @ 16:17:58.191 agent.ephemeral_id: 2afa0e25-7d9e-425a-889a-2572b5b62281 agent.name: ssh-server-4 agent.hostname: web-server agent.version: 7.2.0 agent.type: filebeat agent.id: e3b4065f-2eee-40fe-8ab1-b16f97b77754 sshd_auth_type: password host.hostname: web-server host.os.kernel: 4.15.0-54-generic host.os.name: Ubuntu host.os.family: debian host.os.platform: ubuntu host.os.version: 16.04.6 LTS (Xenial Xerus) host.os.codename: xenial

> Jul 8, 2019 @ 16:17:57.246 sshd_conn_stat: Accepted sshd_user: administrator tags: beats_input_codec_plain_applied sshd_protocol: ssh2 @timestamp: Jul 8, 2019 @ 16:17:57.246 agent.ephemeral_id: f031fd35-8302-41a1-ab00-c0e2637ba894 agent.name: ssh-server-5 agent.hostname: mail-server agent.version: 7.2.0 agent.type: filebeat agent.id: 0ae30e33-add1-4819-a354-220d70cf390a sshd_auth_type: password host.hostname: mail-server host.os.kernel: 4.15.0-54-generic host.os.name: Ubuntu host.os.family: debian host.os.platform: ubuntu host.os.version: 16.04.6 LTS (Xenial Xerus) host.os.codename: xenial

> Jul 8, 2019 @ 16:16:36.178 sshd_conn_stat: Accepted sshd_user: administrator tags: beats_input_codec_plain_applied sshd_protocol: ssh2 @timestamp: Jul 8, 2019 @ 16:16:36.178 agent.ephemeral_id: ee135664-8c38-4aa2-b559-522f2296a188 agent.name: ssh-server-3 agent.hostname: file-server agent.version: 7.2.0 agent.type: filebeat agent.id: f70ce424-f108-4203-855c-9a0c7bf7478d sshd_auth_type: password host.hostname: file-server host.os.kernel: 4.15.0-54-generic host.os.name: Ubuntu host.os.family: debian host.os.platform: ubuntu host.os.version: 16.04.6 LTS (Xenial Xerus) host.os.codename: xenial

Step 4: Open the last document and retrieve the 'host.name' field value.

t	host.name	ssh-server-3
t	host.os.codename	xenial
t	host.os.family	debian
t	host.os.kernel	4.15.0-54-generic
t	host.os.name	Ubuntu

Step 5: Apply the following filter to show all the logs where “host.name” field is “ssh-server-3” and the SSH server IP exists.

Filter: host.name : "ssh-server-3" and sshd_listen_ip : *

Step 6: Open any of the documents and check the sshd_listen_ip field.

t	message	Jul 8 16:19:48 ssh-server-3 sshd[996]: Connection from 192.148.107.6 port 48526 on 192.148.107.3 port 3603
t	sshd_client_ip	192.148.107.6
t	sshd_listen_ip	192.148.107.3
t	sshd_listen_port	3603

The server with IP address 192.148.107.3 got compromised first.

References:

1. ELK Stack (https://www.elastic.co/elk-stack)