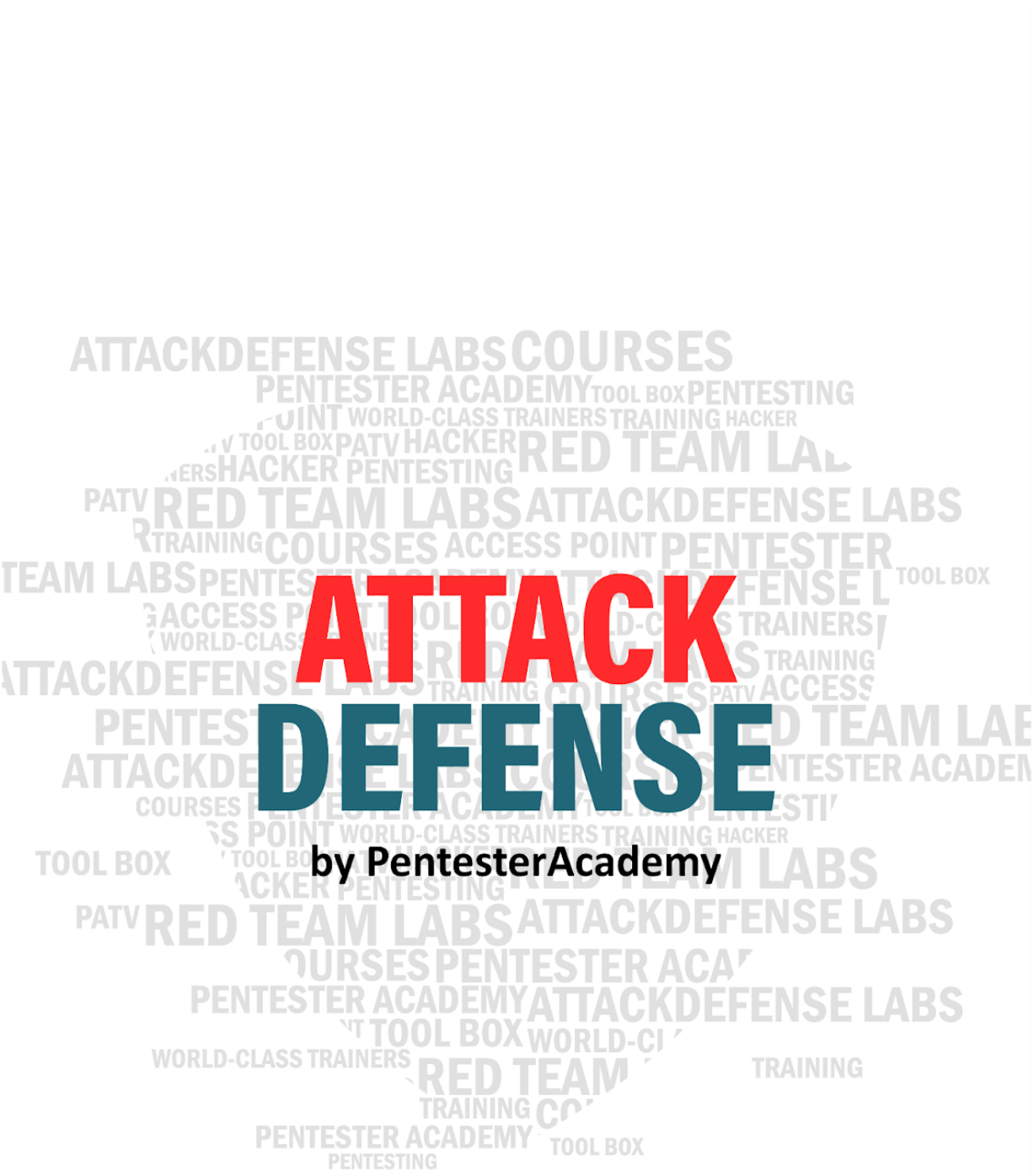
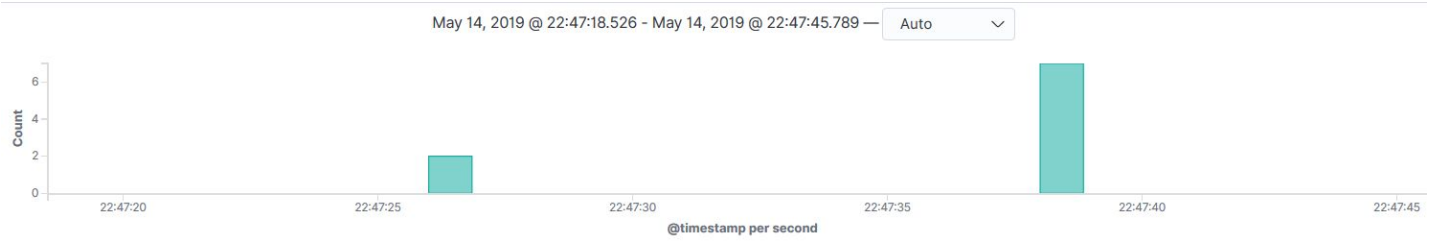

ATTACK
DEFENSE
by PentesterAcademy

Name	Kibana : Windows Event Logs II
URL	https://attackdefense.com/challengedetails?cid=1185
Type	Log Analysis : Windows Event Logs

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 Dashboard:



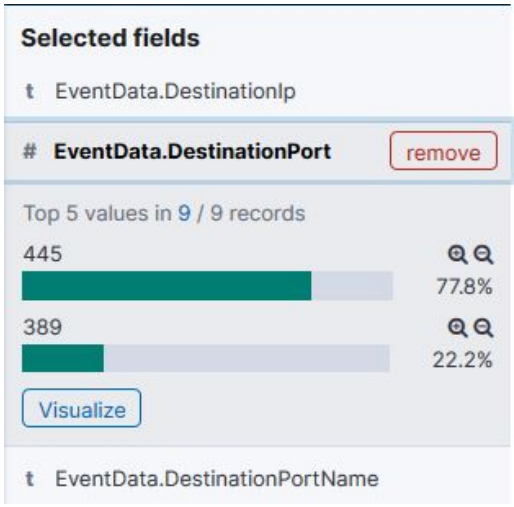
Time	EventData.SourceHostname	EventData.SourceIp	EventData.SourcePort	EventData.DestinationIp	EventData.DestinationPort	EventData.DestinationPortName
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,586	10.59.4.24	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,587	10.59.4.21	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,588	10.59.4.22	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,589	10.59.4.25	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,590	10.59.4.11	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,592	10.59.4.23	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,593	10.59.4.12	445	microsoft-ds
May 14, 2019 @ 22:47:26.000	alice.insecurebank.local	10.59.4.20	49,583	10.59.4.11	389	ldap
May 14, 2019 @ 22:47:26.000	alice.insecurebank.local	10.59.4.20	49,584	10.59.4.11	389	ldap

Q1. A set of machines have been configured to run a file sharing service. One of the machines listened on two different ports to provide access to its files and directories. What was the IP address of that machine?

Answer: 10.59.4.11

Solution:

Step 1: Observe the possible values for destination port field in the Selected fields section on the left panel.



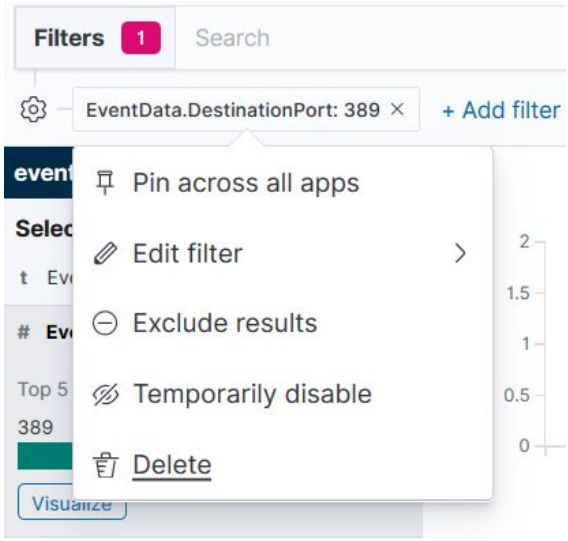
There were two distinct values for destination port field, namely 389 and 445.

Step 2: Click on the zoom-in icon for port 389 and check the values of destination IP address.

EventData.SourceHostname	EventData.SourceIp	EventData.SourcePort	EventData.DestinationIp	EventData.DestinationPort	EventData.DestinationPortName
alice.insecurebank.local	10.59.4.20	49,583	10.59.4.11	389	ldap
alice.insecurebank.local	10.59.4.20	49,584	10.59.4.11	389	ldap

The machine at "10.59.4.11" had a file sharing service running on port 389.

Note: To exit out of the filter, delete the applied filter.



Step 3: Click on the zoom-in icon for port 445 and check the values of destination IP address.

Time	EventData.SourceHostname	EventData.SourceIp	EventData.SourcePort	EventData.DestinationIp	EventData.DestinationPort	EventData.DestinationPortName
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,586	10.59.4.24	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,587	10.59.4.21	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,588	10.59.4.22	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,589	10.59.4.25	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,590	10.59.4.11	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,592	10.59.4.23	445	microsoft-ds
May 14, 2019 @ 22:47:38.000	alice.insecurebank.local	10.59.4.20	49,593	10.59.4.12	445	microsoft-ds

The common destination IP address among both the results is "10.59.4.11".

Alternatively, since the number of event logs are very less in this scenario, a manual search could also be done.

EventData.SourceIp	EventData.SourcePort	EventData.DestinationIp	EventData.DestinationPort	EventData.DestinationPortName
10.59.4.20	49,586	10.59.4.24	445	microsoft-ds
10.59.4.20	49,587	10.59.4.21	445	microsoft-ds
10.59.4.20	49,588	10.59.4.22	445	microsoft-ds
10.59.4.20	49,589	10.59.4.25	445	microsoft-ds
10.59.4.20	49,590	10.59.4.11	445	microsoft-ds
10.59.4.20	49,592	10.59.4.23	445	microsoft-ds
10.59.4.20	49,593	10.59.4.12	445	microsoft-ds
10.59.4.20	49,583	10.59.4.11	389	ldap
10.59.4.20	49,584	10.59.4.11	389	ldap

The machine having IP address "10.59.4.11" listened on two different ports, namely 389 and 445 to provide access to its files and directories.

Q2. How many distinct file sharing servers did the host machine connected to?

Answer: 7

Solution:

Approach 1: Using elasticsearch query.

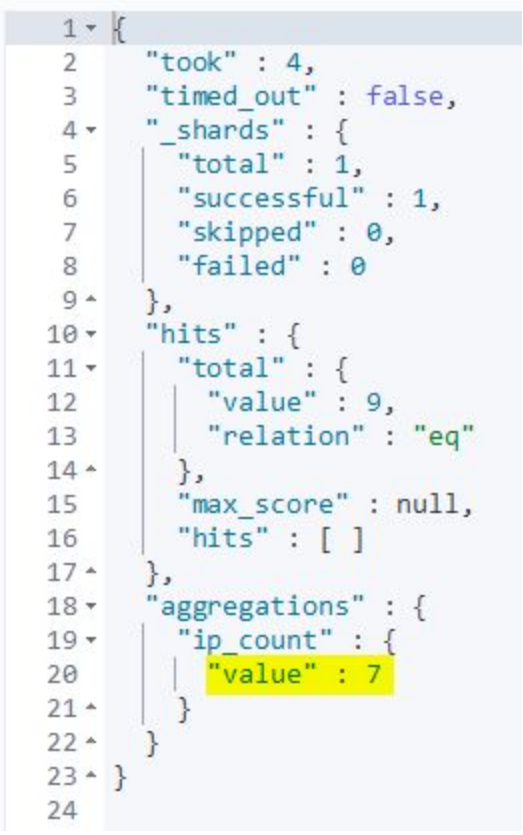
Step 1: Navigate to the "Dev Tools" section available on the left panel.

Step 2: Paste the following query in the console window to get the count of the unique destination IP addresses to which the host machine connected.

Query:

```
GET event-logs/_search
{
  "size": 0,
  "aggs": {
            "ip_count": {
            "cardinality": {
            "field": "EventData.DestinationIp.keyword"
            }
            }
  }
}
```

Press the "Run" button and check the result.



There were 7 distinct destination IP addresses to which the host machine connected.

Approach 2: Counting the distinct IP addresses manually.

Since the number of event logs are very less in this scenario, distinct IP addresses could also be counted manually.

EventData.SourceIp	EventData.SourcePort	EventData.DestinationIp	EventData.DestinationPort	EventData.DestinationPortName
10.59.4.20	49,586	10.59.4.24	445	microsoft-ds
10.59.4.20	49,587	10.59.4.21	445	microsoft-ds
10.59.4.20	49,588	10.59.4.22	445	microsoft-ds
10.59.4.20	49,589	10.59.4.25	445	microsoft-ds
10.59.4.20	49,590	10.59.4.11	445	microsoft-ds
10.59.4.20	49,592	10.59.4.23	445	microsoft-ds
10.59.4.20	49,593	10.59.4.12	445	microsoft-ds
10.59.4.20	49,583	10.59.4.11	389	ldap
10.59.4.20	49,584	10.59.4.11	389	ldap

There were 7 unique destination IP addresses to which the host machine connected.

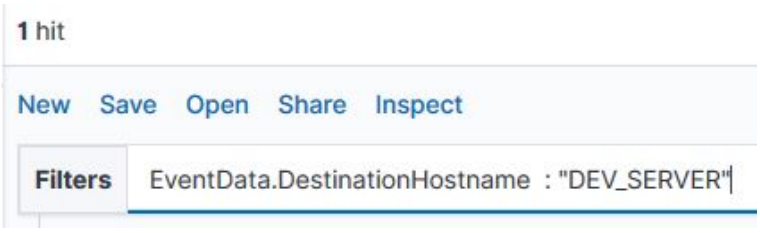
Q3. A file sharing service was running on a machine with the hostname 'DEV_SERVER'. What was the IP address of that machine?

Answer: 10.59.4.12

Solution:

Step 1: Apply the following filter to list all the event logs in which the destination hostname was "DEV_SERVER".

Filter: EventData.DestinationHostname : "DEV_SERVER"



One event log matched the filter.

Step 2: Retrieve the destination IP address from the event log entry that was returned.

EventData.SourceIp	EventData.SourcePort	EventData.DestinationIp	EventData.DestinationPort	EventData.DestinationPortName
10.59.4.20	49,593	10.59.4.12	445	microsoft-ds

The IP address of the file sharing server with hostname "DEV_SERVER" was "10.59.4.12".

References:

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