Activity Tasks

Expand the provided activity files to complete each task. These tasks can be completed in any order.

SSH Barrage

Task: Generate a high amount of failed SSH login attempts and verify that Kibana is picking up this activity.

Activity File: SSH Barrage

Scenario

- You are a cloud architect that has been tasked with setting up an ELK server to gather logs for the Incident Response team to use for training.

- Before you hand over the server to the IR team, your senior architect has asked you to verify the ELK server is working as expected and pulling both logs and metrics from the pentesting web servers.

Your Task: Generate a high amount of failed SSH login attempts and verify that Kibana is picking up this activity.

```
RedAdmin@Jump-Box-Provisioner: ~
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '10.0.0.8' (ECDSA) to the list of known hosts.
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@Jump-Box-Provisioner:~$ for i in {1..5} do ssh RedAdmin@10.0.0.8; done
-bash: syntax error near unexpected token `done'
RedAdmin@Jump-Box-Provisioner:~$ for i in {1..5} do ssh RedAdmin@10.0.0.8;done
-bash: syntax error near unexpected token `done'
RedAdmin@Jump-Box-Provisioner:~$ for i in {1..5} do ssh RedAdmin@10.0.0.8;
> exit
-bash: syntax error near unexpected token `exit'
RedAdmin@Jump-Box-Provisioner:~$ clear
RedAdmin@Jump-Box-Provisioner:~$ while :; do ssh RedAdmin@10.0.0.8; done
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
RedAdmin@10.0.0.8: Permission denied (publickey).
```

Stream Settings

agent.hostname:"Web-1" Customize Highlights 08/09/2021 12:51:47 AM

Aug 9, 2021	event.dataset	Message
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59322 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59324 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59326 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59328 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59330 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59332 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59334 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59336 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59338 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59340 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59342 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59344 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59346 [preauth]
00:51:47.000	system.auth	Connection closed by authenticating user RedAdmin 10.0.0.4 port 59348 [preauth]

No additional entries found. Load again

Linux Stress

Task: Generate a high amount of CPU usage on the pentesting machines and verify that Kibana picks up this data.

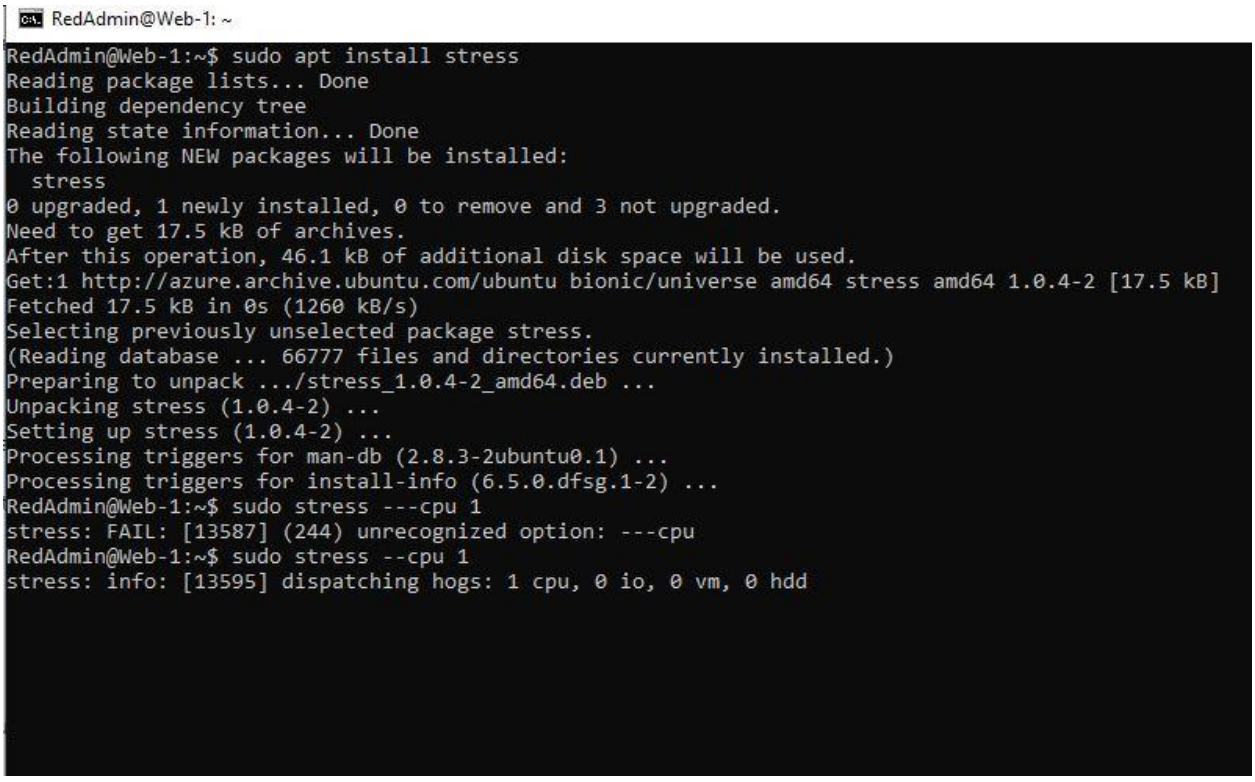
Activity File: Linux Stress

Scenario

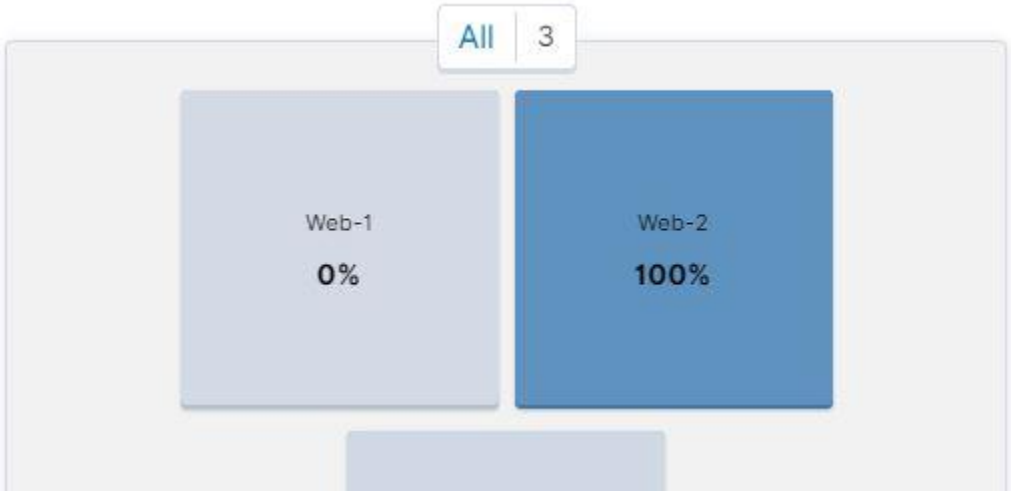
- You are a cloud architect that has been tasked with setting up an ELK server to gather logs for the Incident Response team to use for training.

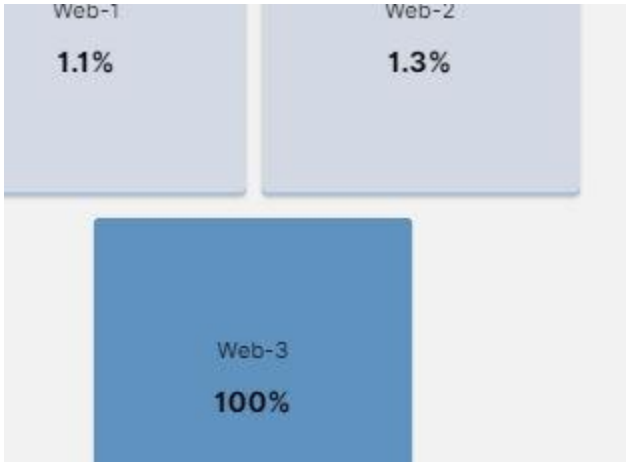
- Before you hand over the server to the IR team, your senior architect has asked that you verify the ELK server is working as expected and pulling both logs and metrics from the pen-testing web servers.

Your Task: Generate a high amount of CPU usage on the pentesting machines and verify that Kibana picks up this data.



Showin





Notes

The Metrics page for a single VM shows the CPU usage for that machine. This shows how much work the machine is doing. Excessively high CPU usage is typically a cause for concern, as overworked computers are at greater risk for failure.

- Metricbeat forwards data about CPU load to Elasticsearch, which can be visualized with Kibana.

- In this activity, you will intentionally stress the CPU of one of your VMs, then find evidence of the increased activity in Kibana.

Linux has a common, easy-to-use diagnostic program called stress. It is easy to use and can be downloaded via apt.

wget-DoS

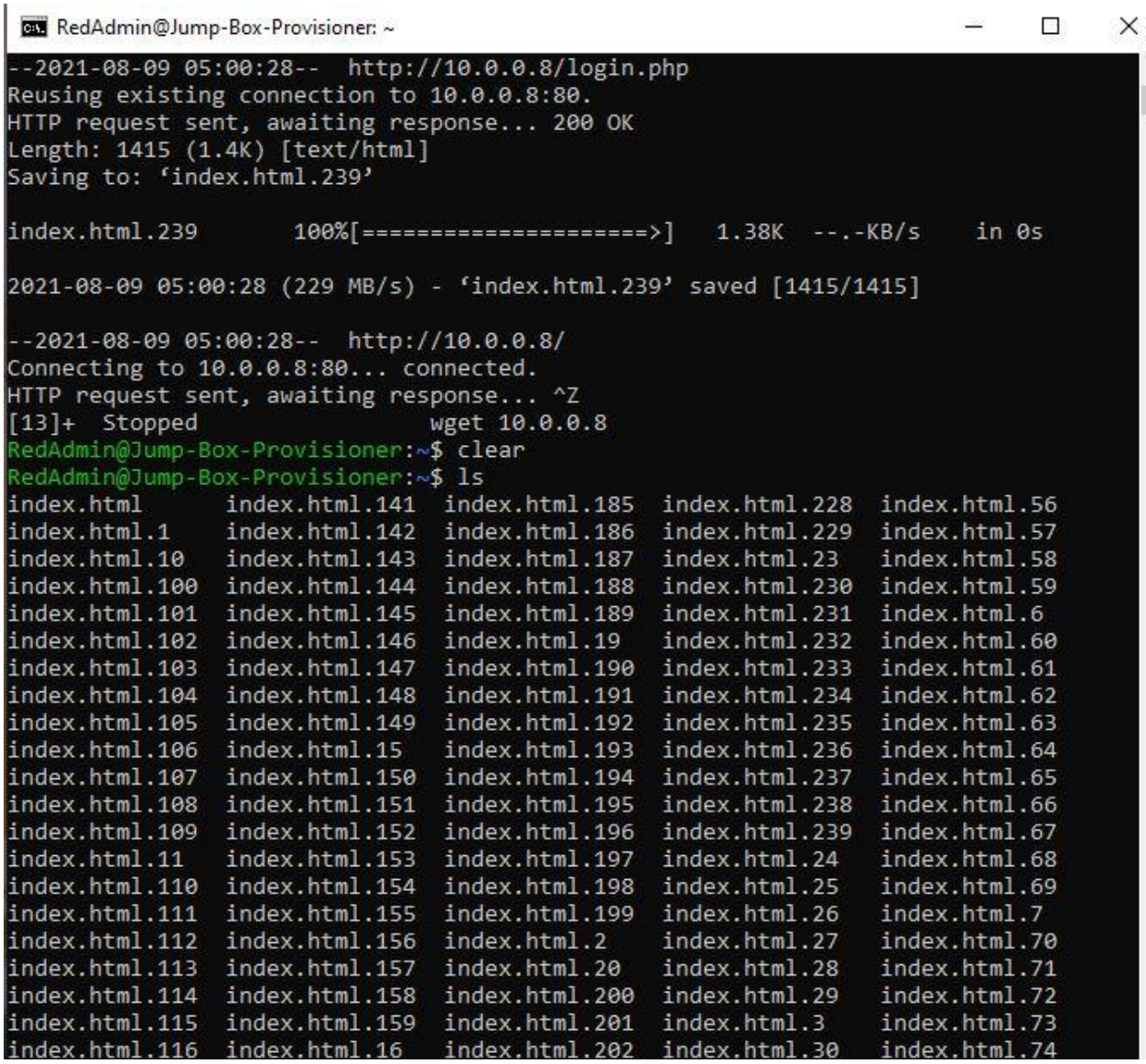
Task: Generate a high amount of web requests to your pen-testing servers and make sure that Kibana is picking them up.

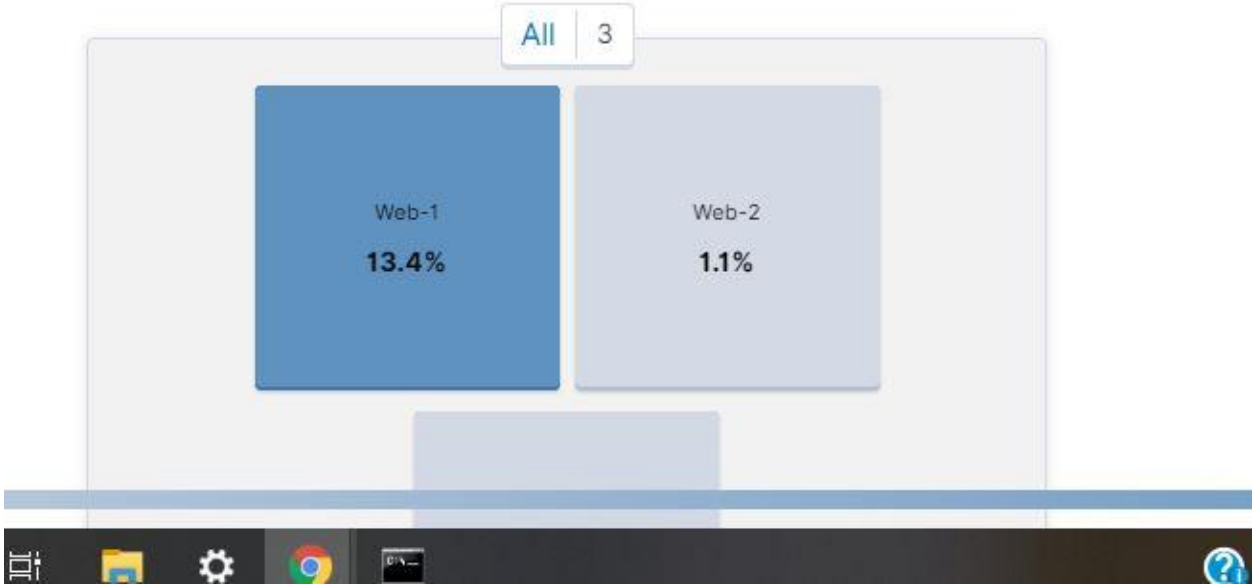
Activity File: wget-DoS

Scenario

- You are a cloud architect that has been tasked with setting up an ELK server to gather logs for the Incident Response team to use for training.

- Before you hand over the server to the IR team, your senior architect has asked that you verify the ELK server is working as expected and pulling both logs and metrics from the pen-testing web servers.






```
index.html.1455  index.html.1926  index.html.2397  index.html.516   index.html.988
index.html.1456  index.html.1927  index.html.2398  index.html.517   index.html.989
index.html.1457  index.html.1928  index.html.2399  index.html.518   index.html.99
index.html.1458  index.html.1929  index.html.24    index.html.519   index.html.990
index.html.1459  index.html.193   index.html.240   index.html.52    index.html.991
index.html.146   index.html.1930  index.html.2400  index.html.520   index.html.992
index.html.1460  index.html.1931  index.html.2401  index.html.521   index.html.993
index.html.1461  index.html.1932  index.html.2402  index.html.522   index.html.994
index.html.1462  index.html.1933  index.html.2403  index.html.523   index.html.995
index.html.1463  index.html.1934  index.html.2404  index.html.524   index.html.996
index.html.1464  index.html.1935  index.html.2405  index.html.525   index.html.997
index.html.1465  index.html.1936  index.html.2406  index.html.526   index.html.998
index.html.1466  index.html.1937  index.html.2407  index.html.527   index.html.999
index.html.1467  index.html.1938  index.html.2408  index.html.528
index.html.1468  index.html.1939  index.html.2409  index.html.529
RedAdmin@Jump-Box-Provisioner:~$ while :; do rm index.html*; done
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
rm: cannot remove 'index.html*': No such file or directory
```