

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).
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

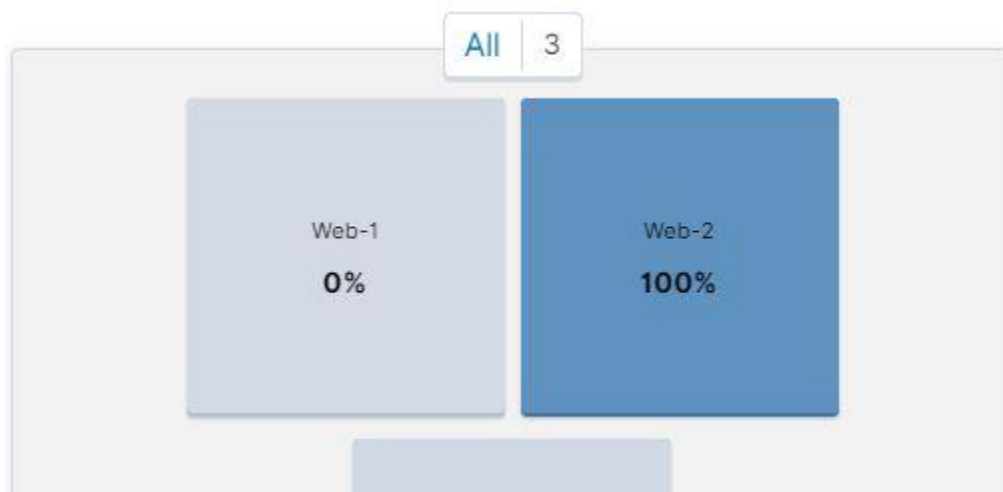
Scenario

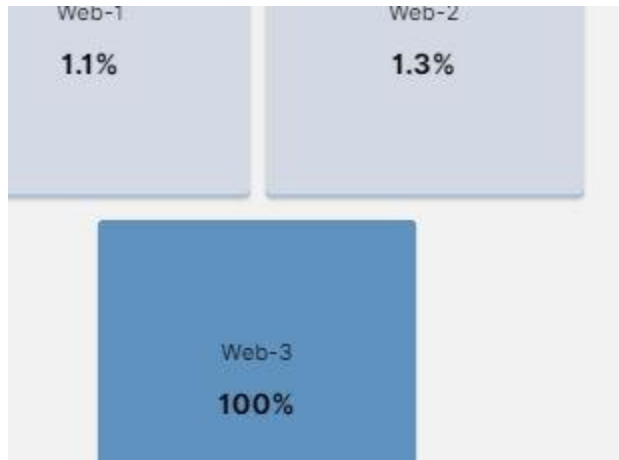
- You are a cloud architect that has been tasked with setting up an ELK server to gather logs for the Incident Response team to use for training.
- Before you hand over the server to the IR team, your senior architect has asked that you verify the ELK server is working as expected and pulling both logs 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.

```
RedAdmin@Web-1: ~  
RedAdmin@Web-1:~$ sudo apt install stress  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following NEW packages will be installed:  
  stress  
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.  
Need to get 17.5 kB of archives.  
After this operation, 46.1 kB of additional disk space will be used.  
Get:1 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 stress amd64 1.0.4-2 [17.5 kB]  
Fetched 17.5 kB in 0s (1260 kB/s)  
Selecting previously unselected package stress.  
(Reading database ... 66777 files and directories currently installed.)  
Preparing to unpack .../stress_1.0.4-2_amd64.deb ...  
Unpacking stress (1.0.4-2) ...  
Setting up stress (1.0.4-2) ...  
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...  
Processing triggers for install-info (6.5.0.dfsg.1-2) ...  
RedAdmin@Web-1:~$ sudo stress ---cpu 1  
stress: FAIL: [13587] (244) unrecognized option: ---cpu  
RedAdmin@Web-1:~$ sudo stress --cpu 1  
stress: info: [13595] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
```

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.

```

RedAdmin@Jump-Box-Provisioner: ~
--2021-08-09 05:00:28-- http://10.0.0.8/login.php
Reusing existing connection to 10.0.0.8:80.
HTTP request sent, awaiting response... 200 OK
Length: 1415 (1.4K) [text/html]
Saving to: 'index.html.239'

index.html.239      100%[=====>]  1.38K  --.-KB/s    in 0s

2021-08-09 05:00:28 (229 MB/s) - 'index.html.239' saved [1415/1415]

--2021-08-09 05:00:28-- http://10.0.0.8/
Connecting to 10.0.0.8:80... connected.
HTTP request sent, awaiting response... ^Z
[13]+  Stopped                  wget 10.0.0.8
RedAdmin@Jump-Box-Provisioner:~$ clear
RedAdmin@Jump-Box-Provisioner:~$ ls
index.html      index.html.141  index.html.185  index.html.228  index.html.56
index.html.1    index.html.142  index.html.186  index.html.229  index.html.57
index.html.10   index.html.143  index.html.187  index.html.23   index.html.58
index.html.100  index.html.144  index.html.188  index.html.230  index.html.59
index.html.101  index.html.145  index.html.189  index.html.231  index.html.6
index.html.102  index.html.146  index.html.19   index.html.232  index.html.60
index.html.103  index.html.147  index.html.190  index.html.233  index.html.61
index.html.104  index.html.148  index.html.191  index.html.234  index.html.62
index.html.105  index.html.149  index.html.192  index.html.235  index.html.63
index.html.106  index.html.15   index.html.193  index.html.236  index.html.64
index.html.107  index.html.150  index.html.194  index.html.237  index.html.65
index.html.108  index.html.151  index.html.195  index.html.238  index.html.66
index.html.109  index.html.152  index.html.196  index.html.239  index.html.67
index.html.11   index.html.153  index.html.197  index.html.24   index.html.68
index.html.110  index.html.154  index.html.198  index.html.25   index.html.69
index.html.111  index.html.155  index.html.199  index.html.26   index.html.7
index.html.112  index.html.156  index.html.2    index.html.27   index.html.70
index.html.113  index.html.157  index.html.20   index.html.28   index.html.71
index.html.114  index.html.158  index.html.200  index.html.29   index.html.72
index.html.115  index.html.159  index.html.201  index.html.3    index.html.73
index.html.116  index.html.16   index.html.202  index.html.30   index.html.74

```

