I first connected to my jumpbox, through

ssh azureuser@40.112.169.59

Last login: Fri May 28 17:10:21 2021 from 100.15.1.253

\*\*\*\*azureuser@Jump-Box:~$ sudo docker container list -a

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

9df70ec7cffb cyberxsecurity/ansible "bash" 2 weeks ago Exited (0) 24 hours ago naughty\_wilbur

azureuser@Jump-Box:~$ sudo docker start naughty\_wilbur

naughty\_wilbur

azureuser@Jump-Box:~$ cd /etc/ansible

-bash: cd: /etc/ansible: No such file or directory

azureuser@Jump-Box:~$ sudo docker attach naughty\_wilbur

root@9df70ec7cffb:~# cd /etc/ansible

root@9df70ec7cffb:/etc/ansible# ansible-playbook install-elk.yml

PLAY [Configure Elk VM with Docker] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TASK [Gathering Facts] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.1.0.4]

TASK [Enable service docker on boot] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.1.0.4]

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.1.0.4 : ok=8 changed=1 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

\*\*\*\*root@9df70ec7cffb:/etc/ansible# ssh azureuser@10.1.0.4

Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1047-azure x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Sat May 29 17:11:45 UTC 2021

System load: 0.36 Processes: 152

Usage of /: 23.5% of 28.90GB Users logged in: 0

Memory usage: 70% IP address for eth0: 10.1.0.4

Swap usage: 0% IP address for docker0: 172.17.0.1

\* Super-optimized for small spaces - read how we shrank the memory

footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

\* Canonical Livepatch is available for installation.

- Reduce system reboots and improve kernel security. Activate at:

https://ubuntu.com/livepatch

10 updates can be applied immediately.

1 of these updates is a standard security update.

To see these additional updates run: apt list --upgradable

New release '20.04.2 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Sat May 29 17:07:44 2021 from 10.0.0.4

azureuser@Web-Elk:~$ sudo snap install nmap

TASK [Install docker.io] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.1.0.4]

To see these additional updates run: apt list --upgradable

New release '20.04.2 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Sat May 29 17:07:44 2021 from 10.0.0.4

THEN WE INSTALLED NMAP; WHICH IS A NETWORK SCANNING TOOL THAT USES IP PACKETS TO IDENTIFY ALL THE DEVICES CONNECTED TO A NETWORK AND TO PROVIDE INFORMATION ON THE SERVICES AND OPERATING SYSTEMS THEY ARE RUNNING.

\*\*\*\*azureuser@Web-Elk:~$ sudo snap install nmap

snap "nmap" is already installed, see 'snap help refresh'

\*\*\*\*azureuser@Web-Elk:~$ nmap -Pn 80 20.185.102.105

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-29 17:15 UTC

Nmap scan report for 80 (0.0.0.80)

Host is up.

All 1000 scanned ports on 80 (0.0.0.80) are filtered

Nmap scan report for 20.185.102.105

Host is up (0.0020s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

22/tcp open ssh

Nmap done: 2 IP addresses (2 hosts up) scanned in 9.32 seconds

azureuser@Web-Elk:~$ sudo docker ps

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

abfcfd13918b sebp/elk:761 "/usr/local/bin/star…" 9 days ago Up 12 minutes 0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp elk

e85d5bbd8214 cyberxsecurity/dvwa "/main.sh" 9 days ago Up 53 minutes 0.0.0.0:80->80/tcp dvwa

azureuser@Web-Elk:~$ curl <http://localhost:5601/app/kibana>

etadata><div class="kibanaWelcomeView" id="kbn\_loading\_message" style="display:none" data-test-subj="kbnLoadingMessage"><div class="kibanaLoaderWrap"><div class="kibanaLoader"></div><div class="kibanaWelcomeLogoCircle"><div class="kibanaWelcomeLogo"></div></div></div><div class="kibanaWelcomeText" data-error-message="Kibana did not load properly. Check the server output for more information.">Loading Kibana</div></div><div class="kibanaWelcomeView" id="kbn\_legacy\_browser\_error" style="display:none"><div class="kibanaLoaderWrap"><div class="kibanaWelcomeLogoCircle"><div class="kibanaWelcomeLogo"></div></div></div><h2 class="kibanaWelcomeTitle">Please upgrade your browser</h2><div class="kibanaWelcomeText">This Kibana installation has strict security requirements enabled that your current browser does not meet.</div></div><script>

// Since this is an unsafe inline script, this code will not run

// in browsers that support content security policy(CSP). This is

// intentional as we check for the existence of \_\_kbnCspNotEnforced\_\_ in

// bootstrap.

window.\_\_kbnCspNotEnforced\_\_ = true;

</script><script src="/bundles/app/kibana/bootstrap.js"></script></body></html>azureuser@Web-Elk:~$

current browser does not meet.</div></div><script>

// Since this is an unsafe inline script, this code will not run

// in browsers that support content security policy(CSP). This is

// intentional as we check for the existence of \_\_kbnCspNotEnforced\_\_ in

// bootstrap.

window.\_\_kbnCspNotEnforced\_\_ = true;

</script><script src="/bundles/app/kibana/bootstrap.js"></script></body></html>azureuser@Web-Elk:~$ exit

logout

Connection to 10.1.0.4 closed.

root@9df70ec7cffb:/etc/ansible# exit

exit

\*\*\*\*azureuser@Jump-Box:~$ wget 10.0.0.5

--2021-05-29 17:24:50-- http://10.0.0.5/

Connecting to 10.0.0.5:80... connected.

HTTP request sent, awaiting response... 302 Found

Location: login.php [following]

--2021-05-29 17:24:50-- http://10.0.0.5/login.php

Reusing existing connection to 10.0.0.5:80.

HTTP request sent, awaiting response... 200 OK

Length: 1415 (1.4K) [text/html]

Saving to: ‘index.html’

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

2021-05-29 17:24:50 (201 MB/s) - ‘index.html’ saved [1415/1415]

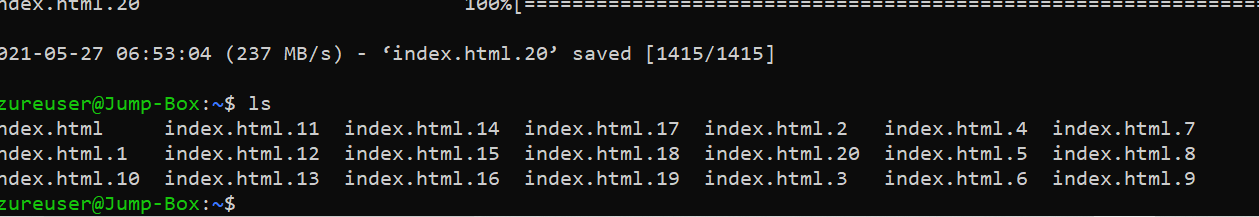
\*\*\*\*Run wget command in a loop to generate web requests on that VM

azureuser@Jump-Box:~$ for i in {1..20}; do ssh azureuser@10.0.0.5; done

\*\*\*\*\*Run the wget command in a loop to generate many web requests

azureuser@Jump-Box:~$ for i in {1..20}; do ssh azureuser@10.0.0.5; ssh azureuser@10.0.0.6; ssh azureuser@10.0.0.8; done

\*\*\*\*ls



\*\*\*\*Write a command to delete all the files at once

rm index.\*

azureuser@Jump-Box:~$ ls

10.0.0.5 index.html

\*\*\*\*\*Find a way to run the wget command without generating these extra files

azureuser@Jump-Box:~$ for i in {1..20}; do wget -p 10.0.0.5; done

\*\*\*\*\*