RedTeam Resource Group

Virtual Network 10.0.0.0/24

Internet

RULE	PORT	PROTOCOL	SOURCE	DESTINATION
Port_22_SSH_Access	22	TCP	0.0.0.0/0	Any
Port_ssh_jumpbox	22	TCP	10.0.0.4	Virtual Network
Port_8080	22	Any	45.72.192.24	Any

RedTeam Security Server/V-Net

Allow SSH from Jumpbox IP

Port 80

20.185.179.54
(RedTeam_PentestLoadBalancer)

Virtual Network 10.0.0.0/24
Subnet 10.1.0.0/24

RULE	PORT	PROTOCOL	SOURCE	DESTINATION
default allow ssh	22	TCP	Any	Any
Port_8080	5601	TCP	45.72.230.103	Any

ELK VM SECURITY GROUP

Connecting Via SSH

Public IP
13.82.110.28

Private IP
10.0.0.4

1. Install Docker io

2. Launching Ansible Container
cyberxsecurity/ansible

3. Launch VM from Azure portal using SSH key from container inside jump box

RedTeamVM /
Jumpbox Provisioner

Port 80

US East

Red Team Load Balancer

access: id_rsa

BEATS

Docker DVWA

Web 1 VM

access: id_rsa

BEATS

Docker DVWA

Web 2 VM

Peering
Red to
Elk

West
US

ELK SERVER   10.1.1.4

HTTP
5601

Filebeat
logs

Ansible Playbook to
install playbook in
Web 1

Connect RedTEam VM
to Web 1 using - SSH

CONNECT VIA
SSH

Laptop

45.72.193.55

Ref: Jumpbox image from: https://www.centrify.com/pam/privileged-access-service/secure-admin-access/