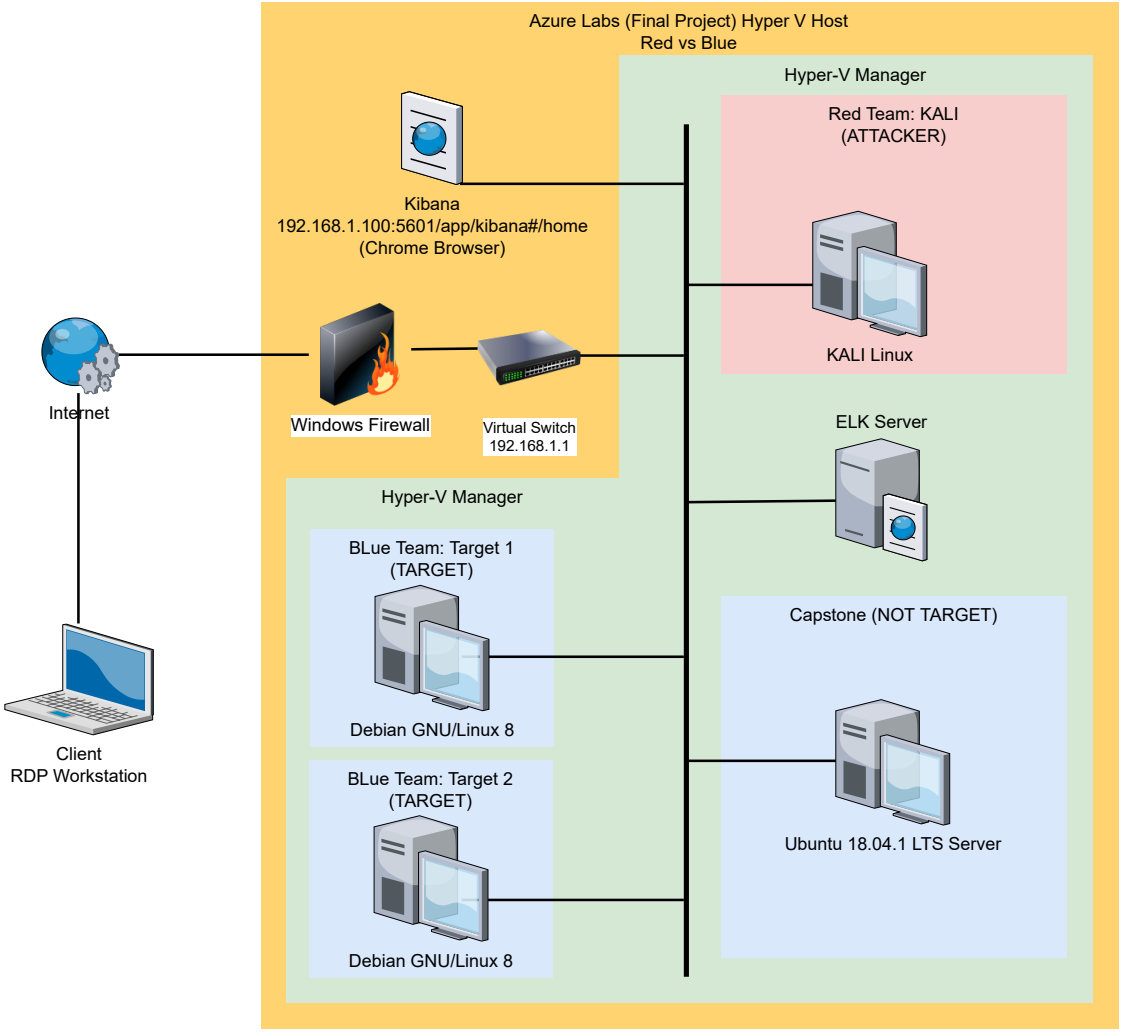
Azure Lab (Final Project): Red vs Blue Network Architecture



Kali (RED TEAM: ATTACKER)

- OS &Version: Kali GNU/Linux 2020.1 (kali-rolling)
- Kernel Version: 5.4.0-kali3-amd64
- IP 192.168.1.90 | 255.255.255.0
- HOST: Kali
- Ports
  - 22/tcp ssh OpenSSH 8.1p1 Debian 5

ELK Server:

- OS & Version: Ubuntu 18.04.4 LTS (Bionic Beaver)
- Kernel Version: 4.15.0-99-generic
- ELK Version 7.6.1
- IP 192.168.1.100 | 255.255.255.0
- MAC: 4C:EB:42:D2:D5:D7
- HOST: ELK
- Ports
  - 22/tcp ssh 7.6p1
  - 9200/tcp Elasticsearch REST API 7.6.1

Kibana (Running on ELK Server)

- Version 7.6.1

Capstone

- OS & Version: Ubuntu 18.04.1 LTS (Bionic Beaver)
- Kernel Version: 4.15.0-108-generic
- IP 192.168.1.105 | 255.255.255.0
- MAC: 00:15:5D:00:04:0F
- HOST: Capstone
- Software **(feeding ELK Server with Data)**
  - filebeat
  - metricbeat
  - packetbeat
- Ports
  - 22/tcp ssh 7.6p1
  - 80/tcp http Apache httpd 2.4.29

General

- Network
  - Address Range: 192.168.1.0/24
  - Subnet Mask: 255.255.255.0
  - Gateways
    - 192.168.1.1
    - 10.0.0.1

Azure Labs Windows

- OS: Microsoft Windows 10 PRO
- OS Version: 10.0.19044 Build 19044
- Virtual Machine
- x64 Desktop
- IP 192.168.1.1 | 255.255.255.0 | MAC: 00-15-5D-00-04-0D
- IP 10.0.0.42 | 255.255.240.0 | MAC: 00-22-48-69-36-2E
- HOST: ML-RefVm-684427
- Ports
  - 135/tcp msrpc
  - 139/tcp netbios-ssn
  - 445/tcp microsft-ds
  - 2179/tcp vmrdp
  - 3389/tcp ms-wbt-server MS Terminal Server

Target 1 (BLUE TEAM: TARGET 1)

- OS & Version: Debian GNU/Linux 8 (jessie)
- Kernel Version: 3.16.0-6-amd64
- IP 192.168.1.110 | 255.255.255.0
- MAC: 00:15:5D:00:04:10
- HOST: TARGET1
- Ports
  - 22/tcp ssh OpenSSH 6.7p1 Debian 5+deb8u4
  - 80/tcp http Apache httpd 2.4.10 ((Debian))
  - 111/tcp rpcbind 2-4 (RPC #100000)
  - 139/tcp netbios-ssn Samba smbd 3.X - 4.X
  - 445/tcp netbios-ssn Samba smbd 3.X - 4.X

Target 2 (BLUE TEAM: TARGET 2)

- OS & Version: Debian GNU/Linux 8 (jessie)
- Kernel Version: 3.16.0-6-amd64
- IP 192.168.1.115 | 255.255.255.0
- MAC: 00:15:5D:00:04:11
- HOST: TARGET1
- Ports
  - 22/tcp ssh OpenSSH 6.7p1 Debian 5+deb8u4
  - 80/tcp http Apache httpd 2.4.10 ((Debian))
  - 111/tcp rpcbind 2-4 (RPC #100000)
  - 139/tcp netbios-ssn Samba smbd 3.X - 4.X
  - 445/tcp netbios-ssn Samba smbd 3.X - 4.X