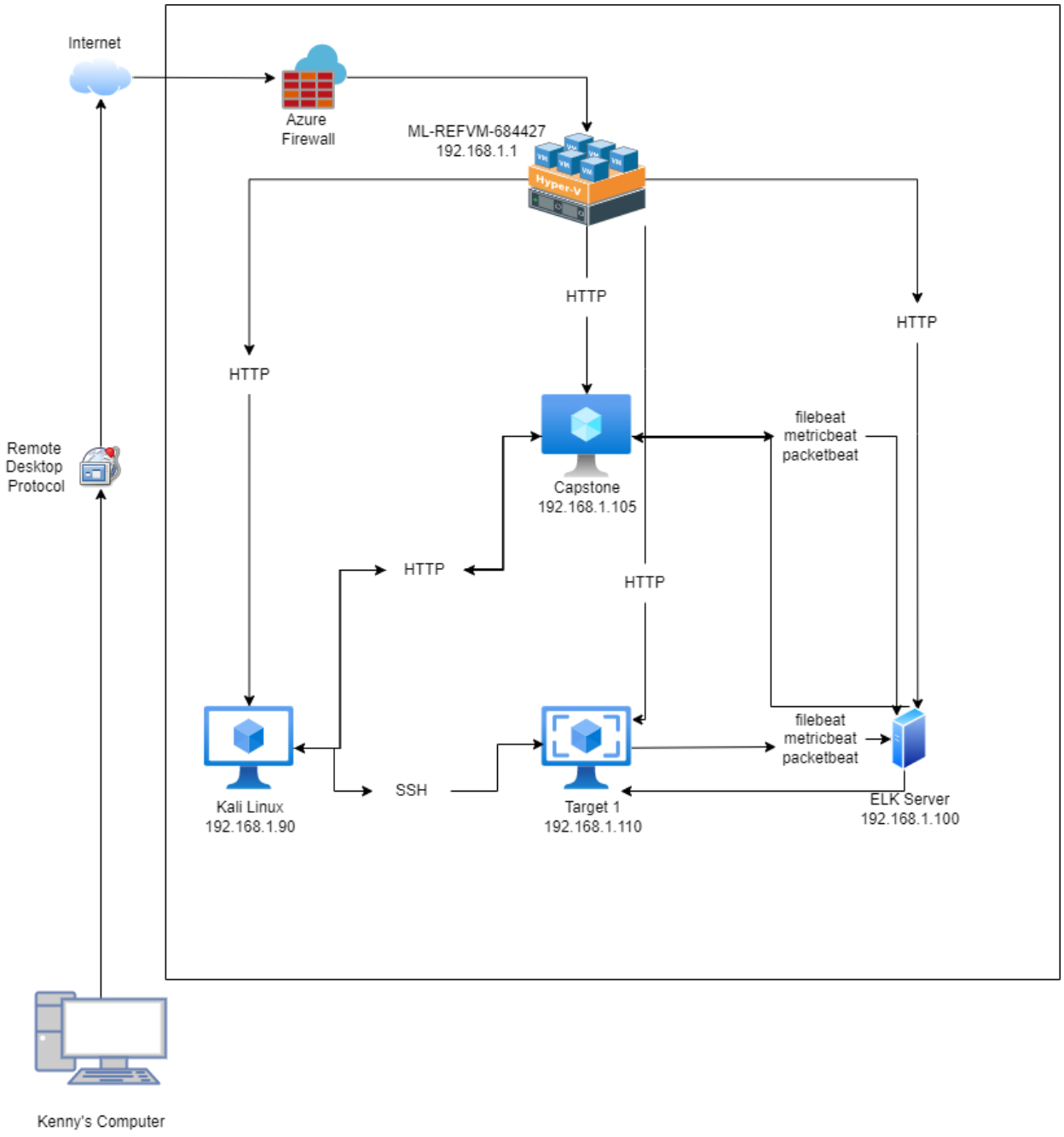
Network Topology

Name of VM 1: Capstone
Operating System: Ubuntu
Purpose: Vulnerable Web Server
IP Address: 192.168.1.105

Name of VM 2: Kali
Operating System: Kali Linux
Purpose: Penetration Tester
IP Address: 192.168.1.90

Name of VM 3: ELK
Operating System: Ubuntu
Purpose: Elasticsearch and Kibana
IP Addres: 192.168.1.100

Name of VM: Target 1
Operating System: Linux
Purpose: Target Machine
IP Address: 192.168.1.110



Description of Targets

The target of this attack was: Target 1 (192.168.1.110)

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Monitoring the Targets

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:
Metric: WHEN count() GROUPED OVER top “http.response.status_code”
Threshold: 400 for the last 5 minutes
Vulnerability Mitigated: Brute Force Attacks and Enumeration
Reliability: It is highly reliable because it filters out normal activity. Codes 400 and above are are client and server error responses which are ones that should be closely monitored especially when there is a higher frequency of them.

CPU Usage Monitor

CPU Usage Monitor is implemented as follows:
Metric: WHEN max() OF “system.process.cpu.total.pct” OVER all documents
Threshold: above 0.5 for the last 5 minutes
Vulnerability Mitigated: possible malware or viruses
Reliability: This is rated medium on reliability. Though this threshold will definitely monitor any suspicious activity, it might also pick up daily activities that might consume more CPU power on occasions.

HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:
Metric: WHEN sum() of http.request.bytes OVER all documents
Threshold: above 3500 for the last minute
Vulnerability Mitigated: Cross Site Scripting or DDos attacks
Reliability: This alert is a medium reliability because it can create false positives. It could be regular use of HTTP requests or traffic.