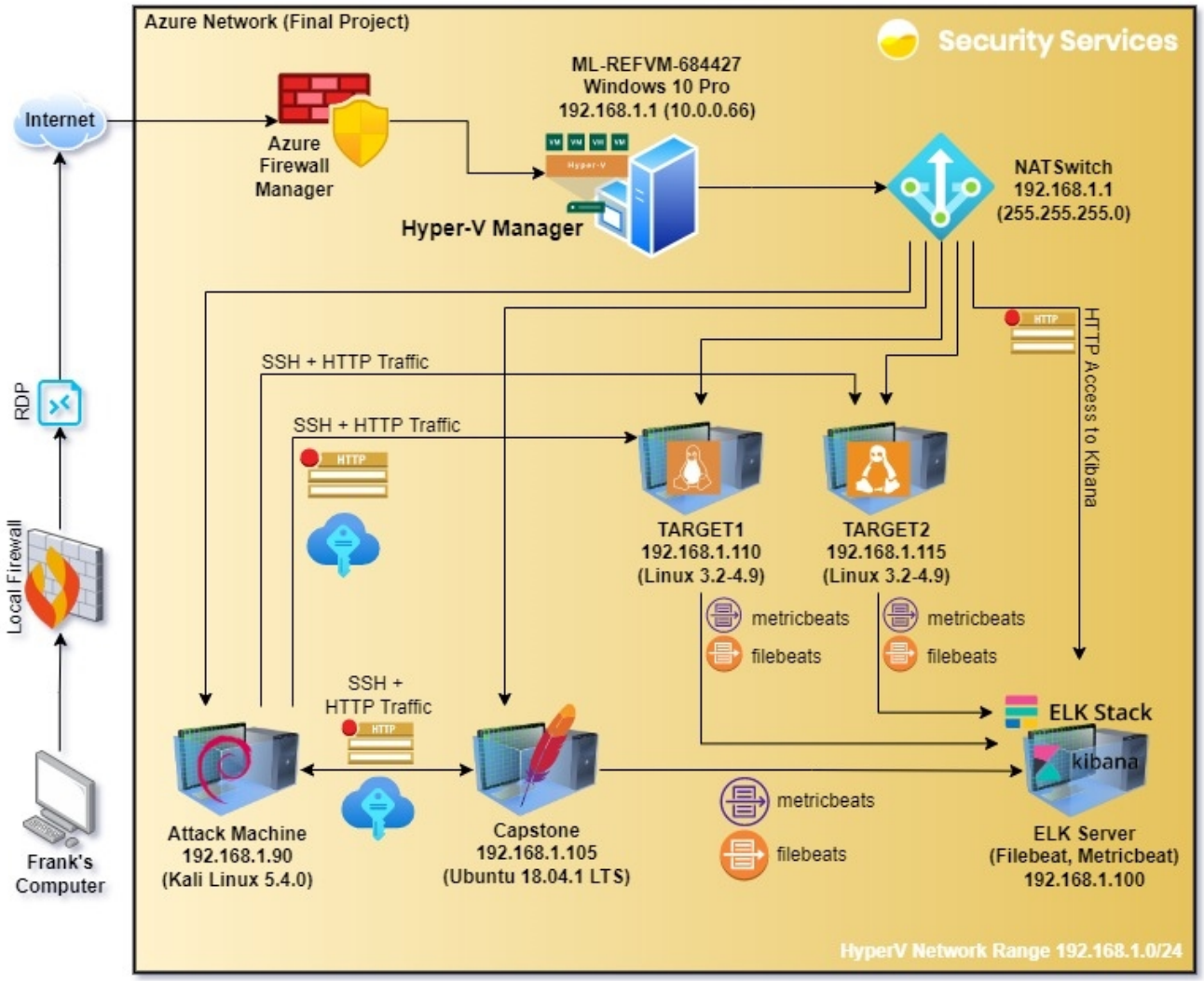
Blue Team: Summary of Operations

Table of Contents

Network Topology



The following machines were identified on the network:

- **HyperV Manager Host (ML-REFVM-684427)**
  - **Operating System**: Microsoft 10 Pro
  - **Purpose**: HyperV Manager Host Machine
  - **IP Address**: 192.168.1.1

- **Capstone**
  - **Operating System**: Ubuntu 18.04.1 LTS server1
  - **Purpose**: Unknown/ Out of Scope
  - **IP Address**: 192.168.1.105

- **ELK**
  - **Operating System**: Ubuntu 18.04.4 LTS
  - **Purpose**: Elasticsearch Logs and Beats Monitoring Machine
  - **IP Address**: 192.168.1.100

- **Kali**
  - **Operating System**: Kali Linux 5.4.0
  - **Purpose**: Attacking Machine
  - **IP Address**: 192.168.1.90

- **TARGET1**
  - **Operating System:** Linux 3.x | 4.x (Linux 3.2 – 4.9)
  - **Purpose**: Victim Machine
  - **IP Address**: 192.168.1.110

- **TARGET2**
  - **Operating System**: Linux 3.x | 4.x (Linux 3.2 – 4.9)
  - **Purpose**: Victim Machine
  - **IP Address**: 192.168.1.115

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 (Apache httpd 2.4.10) and 22 (OpenSSH 6.7p1) 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

```
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
```

Excessive HTTP Errors is implemented as follows:
  - **Metric**: Monitors if the top 5 errors for status codes in the last 5 minutes
  - **Threshold**: Fires off if the “Top 5” HTTP error codes in the last 5 minutes is in the 400 range
  - **Vulnerability Mitigated**: Helps with contributing to preventing Brute Force Attacks with high number of failed login attempts or wrong passwords submitted. High level of traffic from specific IP’s generating 4xx codes can also be blocked by adding to a block list for the source being a possible attacker.

- **Reliability**: This alert has a high reliability as it should only trigger when there is a lot of error activity that seems abnormal trying to access the website from activities such as Brute Force or bad traffic requests in attempts to DDoS the server. All 4xx codes are client error codes, meaning the user accessing the server is making a mistake or sending abnormal/ unauthorized actions.

HTTP Request Size Monitor

```
WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
```

HTTP Request Size Monitor is implemented as follows:
- **Metric**: Monitors for total bytes sent for all documents for the last minute
- **Threshold**: Measures every minute and fires if total is above 3500 bytes
- **Vulnerability Mitigated**: Helps with preventing possible DDoS attacks that would come from attackers making a high amount of traffic reach the site in short amounts of time to slow it down or crash it.
- **Reliability**: This alert may generate a lot of false positives from fast page browsing or higher sized page downloads that have a lot of content that totals over 3500 bytes such as pages with a lot of photos or images used. As a result, it has a low reliability. Reliability could increase if threshold is adjusted to a reasonable level based on “normal” data total behavior.

CPU Usage Monitor

```
WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
```

CPU Usage Monitor is implemented as follows:
- **Metric**: Measures the percentage of CPU usage from system processes in the last 5 minutes
- **Threshold**: Fires off if the total CPU usage is above 50% for all requests processed
- **Vulnerability Mitigated**: Mitigate DDoS attack methods before it impacts system performance.
- **Reliability**: This alert may generate a moderate amount of false positives depending on the traffic hitting the website. If it is under heavy access load, then this alert is not reliable at all as a high number of users simultaneously accessing pages would trigger this alert easily. There are also random system processes or updates that might run in the background that would spike the CPU usage activity above the threshold set.

Suggestions for Going Further (Optional)

- Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a block-list is an effective tactic against brute-force attacks. It is not necessary to explain _*how*_ to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

- Vulnerability 1
- ****Patch****: Implement an NDR system to the network for detecting high level of failed login attempts traffic and flag it for suspicious behavior. Immediately block traffic and add the IP address to a block list for review by a SOC to confirm suspicious behavior.

  - **Why It Works**: Slows down attacker(s) and bad actor(s) ability to try and brute force the system.

- Vulnerability 1 (alternative/ additional)
  - **Patch**: Implement SSH keys for all server logins with users so that logins can be made more securely with validated secure key pairs.
  - **Why It Works**: Completely gets rid of password brute force attempts from unauthorized machines that do not have the key or on the white list of accessible IP addresses. Allows users to not have weak passwords to create or implement while maintaining a more secure validation process for logging in.

- Vulnerability 2
  - **Patch**: TODO: E.g., _*install* `special-security-package` *with* `apt-get`_
  - **Why It Works**: TODO: E.g., _`special-security-package` *scans the system for viruses every day*_

- Vulnerability 3
  - **Patch**: TODO: E.g., _*install* `special-security-package` *with* `apt-get`_
  - **Why It Works**: TODO: E.g., _`special-security-package` *scans the system for viruses every day*_