Network Topology

The following machines were identified on the network:

- Name of VM 1 : Attacking Machine
    - **Operating System**: Linux
    - **Purpose**: To attack target machines.
    - **IP Address**: 192.168.1.90
- Name of VM 2 : Target 1
    - **Operating System**: Linux
    - **Purpose**: Clients Machine
    - **IP Address**: 192.168.1.110
- Name : Target 2
    - **Operating System**: Linux
    - **Purpose**: Clients machine
    - **IP Address**:192.168.1.115
- Name : ELK
    - **Operating System**: Linux
    - **Purpose**: Log manager
    - **IP Address**:192.168.1.100
- Name : Capstone
    - **Operating System**: Linux
    - **Purpose**: Project
    - **IP Address**:192.168.1.105

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

Alert 1 is implemented as follows:

- **Metric**: Packetbeat
- Threshold: WHEN count GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: Lets you if someone is trying to access a hidden directory and if getting 400 and above response codes.
- **Reliability**: Medium reliability

HTTP Request Size Monitor

Alert 2 is implemented as follows:

- **Metric**: Packetbeat
- **Threshold**:WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- **Vulnerability Mitigated**: Informs you if a bruteforce attack or directory traversal is happening. Malicious actors can be using a tool such a Gobuster to Brute force URL's
- **Reliability**: High reliability

CPU Usage Monitor

- **Metric**: Metricbeat
- **Threshold**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: This could detect a failing cpu - mine cryptocurrency,
- **Reliability**: medium

Suggestions for Going Further

- 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 blocklist 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 : Bruteforce attack

    - **Patch**: Apply a WAF (web application firewall), Monitor Location History

- **Why It Works**: A WAF secures a website thoroughly and it stalls the attack from happening. The alert that is set up will let us know to secure the data as soon as possible while the malicious actors try to figure out a way around the WAF. Also if you monitor the location history, you can see any suspicious login requests that are coming from a country that the company's employees do not reside in, so you can be prepared if you are being attacked.

Vulnerability 2 : DDOS Attack

- **Patch**: There are no reliable patches or software updates that have been proven to control DDOS attacks but there are DDoS mitigation services, e.g cloudflare.
- **Why It Works:** Why It Works: DDOS mitigation services, detect suspected DDOS attacks, reroute them, and use machine learning to adapt to the attack pattern. There are so many services offering this real time DDOS protection but for a price of $20/month minimum.

Vulnerability 3 :**CPU Excess Usage**

- **Patch**:
- sudo apt update && sudo apt -y upgrade (Update/Upgrade Software)
- sudo apt purge application (Removing and Reinstalling apps)
- sudo apt update
- sudo apt install application
- **Why It Works**:By using the patch above one can update all the system software. If this does not work then we can move on by uninstalling and reinstalling the given program, to see if the issue was a problem in the way it was originally installed.