**Blue Team: Summary of Operations**

**Table of Contents**

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic & Behavior
* Suggestions for Going Further

**Network Topology**

The following machines were identified on the network:

**Network**

Address Range: **192.168.1/24**

Netmask: **255.255.255.0**

Gateway: **192.168.1.1**

**Machines**

IPv4: **192.168.1.90**

OS: **Linux 2.6.32**

Hostname: **Kali**

IPv4: **192.168.1.100**

OS: **Ubuntu 18.04.01**

Hostname: **ELK**

IPv4: **192.168.1.105**

OS: **Ubuntu 18.04.01**

Hostname: **Capstone**

IPv4: **192.168.1.110**

OS: **Linux 3.2 - 4.9**

Hostname: **Target 1**

IPv4: **192.168.1.115**

OS: **Linux 3.2 - 4.9**

Hostname: **Target 2**

**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 is implemented as follows:

“WHEN count() GROUPED OVER top 5 'http.response.status\_code' IS ABOVE 400 FOR THE LAST 5 minutes”

* **Metric**: Packetbeat - http.response.status\_code > 400
* **Threshold**: Grouped top 5 for the last 5min
* **Vulnerability Mitigated**: This alert is an indication of an attempted brute force in progress.
* **Reliability**: *Medium* ­- This would provider reliable data that alerts you to a brute force withing the last 5 min.

**HTTP Request size Monitor**

Alert is implemented as follows:

“WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute”

* **Metric**: Packetbeat - http.request.bytes > 3500
* **Threshold**: all documents over 3500 bytes in the last 1 minute
* **Vulnerability Mitigated**: This alert is an indication of a DDoS attack in process.
* **Reliability**: *Medium* - This alert should not generate a significant amount of false negatives as this as 3500 is a lot more than what would be considered regular traffic.

**CPU Usage Monitor**

Alert 3 is implemented as follows:

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

* **Metric**: Metricbeat - system.process.cpu.total.pct > 0.5
* **Threshold**: 50% of CPU utilized in the last 5 min.
* **Vulnerability Mitigated**: This alert is an indication of an interaction if malware or virus.
* **Reliability**: *low* - This is still a good alert to detect if your system has encountered malware but you can also hit 50% utilization with a lot of users connecting to your network during peak periods.

**Suggestions for Going Further (Optional)**

* Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behaviour, 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:

* Brute Force Attacks
  + **Patch**: Some options would be to implement an IDS to blacklist certain problems. You could also enforce a cooldown period of 30min for users that have failed the last 5 login attempts.
  + **Why It Works**: This works because a brute force attack will make several login attempts within second, this allows them to try thousands of passwords within minutes. By locking them out after 5 failed attempts drastically increase the time it would take to brute force, making it not feasible.
* DDoS Attacks
  + **Patch**: Implementing an IDS to block multiple requests from the same IP address and disable echo where possible.
  + **Why It Works**: This works by having a system blocking problematic connection points preventing them reconnecting to the network.
* Vulnerability 3
  + **Patch**: Implementing on going training for employees.
  + **Why It Works**: This is not a technical patch but humans are often the weakest link in any network. By increasing training of employees would drastically reduce the likelihood of them clicking on a malicious link or email.