Blue Team: Summary of Operations (DEFENSIVE)

Table of Contents

Network Topology

The following machines were identified on the network:
Azure VM
OS: Windows 10
Purpose: Host
IP Address: 192.168.1.100:5601

ELK
OS: Ubuntu 18.04.4 LTS
Purpose: SIEM
IP Address: 192.168.1.100

Kali
OS: Kali Linux - 5.4.0-kali3-amd64
Purpose: Attacker
IP Address: 192.168.1.90

Capstone
OS: Ubuntu 18.04.1 LTS
Purpose: Server
IP Address: 192.168.1.105

Target 1
OS: Debian GNU/Linux 8
Purpose: Vulnerable WordPress
IP Address: 192.168.1.110

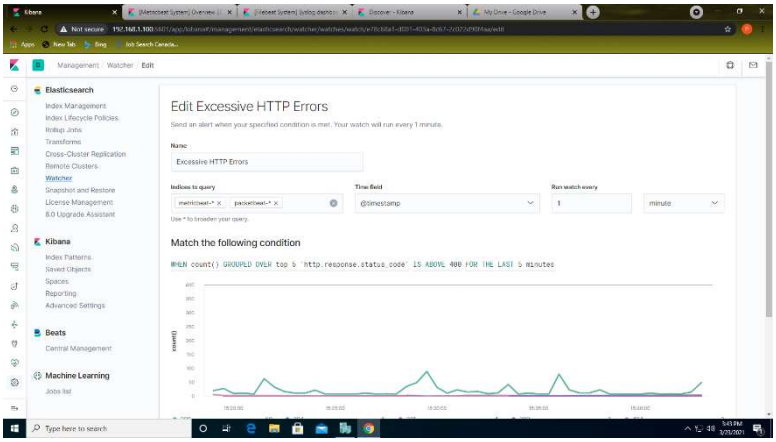
Description of Targets

The target of this attack was: Target 1 - IP Address: 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

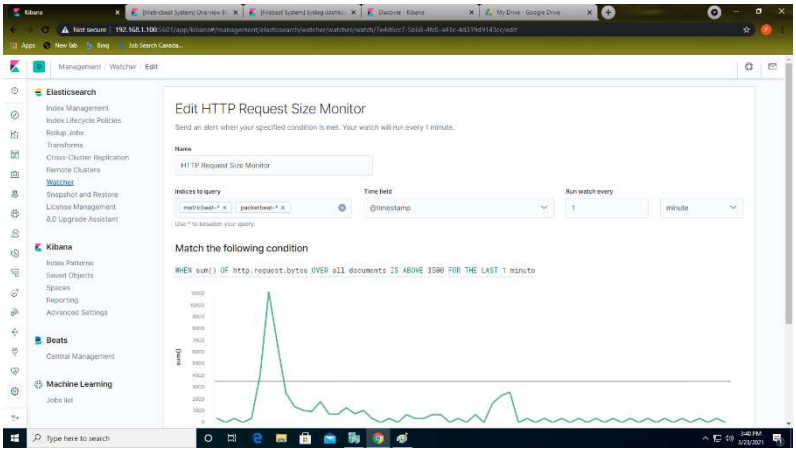
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

Alert 1: Excessive HTTP Errors



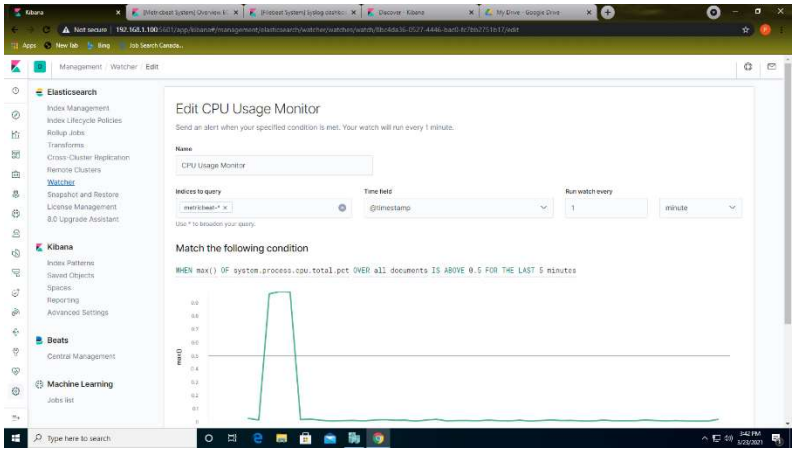
Metric: Metricbeat-* , Packetbeat-*
Threshold: The alert is triggered when the http.response.status.code for the top 5 is above 400 for the last 5 minutes.
Vulnerability Mitigated: Brute Force
Reliability: It is clear that this alert can generate some false positives, therefore it receives a medium reliability rating. Since HTTP response status codes of 400 do not always indicate that a brute force attack is occurring, it is highly likely a brute force attack is happening if there are multiple HTTP response status codes of 400 happening in a very short time frame.

Alert 2: HTTP Request Size Monitor



Metric: Metricbreat-*, Packetbeat-*
Threshold: This alert is triggered when the sum of **http.request.bytes** OVER all documents IS **ABOVE 3500** FOR THE LAST 1 minute
Vulnerability Mitigated: Port Scan - WPScan
Reliability: This alert generates lots of false positives. Rate as low.

Alert 3: CPU Usage Monitor



Metric: Metricbeat-*
Threshold: This alert is triggered WHEN max OF **system.process.cpu.total.pct** OVER all documents IS **ABOVE 0.5** FOR THE LAST 5 minutes.
Vulnerability Mitigated: Brute force, DDoS, and file exfiltration
Reliability: This alert is susceptible to false positives. We would have to take an in-depth snapshot of the company server over a month period to understand the level in which they engage the CPU during that period. The threshold of the alert should then be fine-tuned with a provided baseline taken before establishing the alert to indicate these vulnerabilities.