Blue Team: Summary of Operations

Table of Contents

* Network Topology
* Description of Targets
* Monitoring the Targets

Network Topology

The following machines were identified on the network:

* ML-RefVm-684427
  + **Operating System**: Windows
  + **Purpose**: Host VM
  + **IP Address**: 192.168.1.1
* Kali
  + **Operating System**: Linux
  + **Purpose**: Attacking machine
  + **IP Address**: 192.168.1.90
* Capstone
  + **Operating System**: Linux
  + **Purpose**: Capstone server
  + **IP Address**: 192.168.1.105
* ELK
  + **Operating System**: Linux
  + **Purpose**: Monitoring machine
  + **IP Address**: 192.168.1.100
* Target
  + **Operating System**: Linux
  + **Purpose**: WordPress server
  + **IP Address**: 192.168.1.110

Description of Targets

The target of this attack was: Target 1 - IP: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**: http.response.status\_code
* **Threshold**: IS ABOVE 400
* **Vulnerability Mitigated**: Brute force attack to server
* **Reliability**: Medium
* **Explanation**: Alert 1 triggers when HTTP response code is returned 400 or above, which brute force attacks return error code 401 from my findings. However for this reason, it has been listed as medium reliability due to the fact not all 400 or above error codes are brute force attacks and can return false positives. I have observed code 404 being returned on unresponsive pages or if a webpage path is entered incorrectly.

Alert 2: HTTP Request Size Monitor

* **Metric**: http.request.bytes
* **Threshold**: IS ABOVE 3500
* **Vulnerability Mitigated**: Excessive traffic and/or DDoS attacks
* **Reliability**: Low
* **Explanation**: Alert 2 triggers when the HTTP request bytes exceed 3500 within 1 minute, this allows us to gauge when excessive and/or offensive traffic is being sent to the server. Unfortunately the alert generates a large amount of false positives as they are triggered almost every minute for no reason.

Alert 3: CPU Usage Monitor

* **Metric**: system.process.cpu.total.pct
* **Threshold**: IS ABOVE 0.5
* **Vulnerability Mitigated**: Reverse shell and/or file execution
* **Reliability**: High
* **Explanation**: Alert 3 triggers when the servers processes exceed 0.5. With this alert in place, we will be notified when the server is being utilised more, which in effect should not be the case under normal circumstances as the webserver would not be expected to struggle through normal web browsing.