Blue Team: Summary of Operations

Table of Contents

Network Topology

TODO: Fill out the information below.

The following machines were identified on the network:

- Target 1
  -Linux Kernel
  - Runs Wordpress server on this machine
  - 192.168.1.110
- Kali
  - Linux Kernel
  - Attack machine
  - 192.168.1.90
- ml-refvm-684427
  - Microsoft windows
  - Host Server, NAT switch
  - 192.168.1.1
- Elk
  - Linux kernel
  - log server
  - 192.168.1.100

-capstone
  - Linux kernel
  - capstone server
  - 192.168.1.105

-Target 2
  - Linux Kernel
  - exploitable machine (optional)
  - 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 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 Erros

Excessive HTTP Error is implemented as follows:
- Metric: Packetbeat
- Threshold: 5
- Vulnerability Mitigarted: HTTP response Status code
- Reliability: Medium

HTTP request size Monitor
Alert 2 is implemented as follows:
- Metric: Packetbeat
- Threshold: 3500
- Vulnerability Mitigated HTTP request byte
- Reliability: Medium

CPU usage monitor
Alert 3 is implemented as follows:
- Metric: Metricbeat
- Threshold: Above 0.5
- Vulnerability Mitigated: System process cpu
- Reliability: low