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:
- Capstone
  - **Operating System**:Ubuntu Linux
  - **Purpose**:alert testing/target
  - **IP Address**:192.168.1.105
- ELK
  - **Operating System**:Ubuntu Linux
  - **Purpose**:access via web to view alarts
  - **IP Address**:192.168.1.100
- Kali
  - **Operating System**:Kali Linux
  - **Purpose**:attacking machine/pen test machine
  - **IP Address**:192.168.90
- target 1
  - **Operating System**:Debian linux
  - **Purpose**:vulnerable wordpress
  - **IP Address**:192.168.1.110
- target 2
  - **Operating System**:Debian Linux
  - **Purpose**:vulnerable machine
  - **IP Address**: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 Errors

Alert 1 is implemented as follows:
  - **Metric**: WHEN count()GROUPED OVER top 5

'http.response.status_code'IS ABOVE 400FOR THE LAST 5 minutes
- **Threshold**: above 400
- **Vulnerability Mitigated**: http authentication codes/password fails/brute force
  - **Reliability**: The alert is highly reliable. Measuring by error codes 400 and above will filter out any normal or successful responses. 400+ codes are client and server errors which are of more concern. Especially when taking into account these error codes going off at a high rate.

HTTP request size monitor
Alert 2 is implemented as follows:
  - **Metric**: WHEN sum()OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
  - **Threshold**: 3500 over 1 minute
  - **Vulnerability Mitigated**: Code injection in HTTP requests (XSS and CRLF) or DDOS.
  - **Reliability**: Alert could create false positives. It comes in at a medium reliability. There is a possibility for a large non malicious HTTP request or legitimate HTTP traffic.

CPU usage monitor
Alert 3 is implemented as follows:
  - **Metric**: WHEN max()OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
  - **Threshold**: 0.5 for the last 5 minutes
  - **Vulnerability Mitigated**: malware detection/overuse of resorces.
  - **Reliability**: The alert is highly reliable. Even if there isn’t a malicious program running this can still help determine where to improve on CPU usage.