Blue Team: Summary of Operations

Table of Contents

Network Topology

TODO: Fill out the information below.

The following machines were identified on the network:

- ELK stack
  - **Operating System**: Linux
  - **Purpose**: ELK stack hosting
  - **IP Address**:192.168.1.100
- Kali
  - **Operating System**: Linux
  - **Purpose**:used for the penetration testing
  - **IP Address**: 192.168.1.90
- Capstone
  - **Operating System:** Linux
  - **Purpose:** Filebeat and metric beat are installed and will forward logs to the ELK machine
  - **IP Address:** 192.168.1.105
- Target 1
  - **Operating system:** Linux
  - **Purpose:** exposes vulnerabilities
  - **IP Address:** 192.168.1.110

Description of Targets

TODO: Answer the questions below.

The target of this attack was: Target 1 (TODO: **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:

Name of Alert 1

‘HTTP_Errors’

- **Metric**: HTTP status codes
- **Threshold**: 400 per 5 minutes
- **Vulnerability Mitigated**: DDoS attacks, project reliability
- **Reliability**: Medium - internal issues may arise such as project downtime due to release, not a threat actor that poses a risk to the data being compromised.

Name of Alert 2

HTTP Request Size Monitor: ‘HTTP_Req_Size’

- **Metric**: HTTP req bytes
- **Threshold**: Aggregate all docs size > 3500 bytes
- **Vulnerability Mitigated**: Buffer overflow, DDoS attacks
- **Reliability**: High

Name of Alert 3

CPU Usage Monitor: CPU_Usage

- **Metric**: CPU Usage
- **Threshold**: 0.5/5 mins
- **Vulnerability Mitigated**: DDoS, high traffic volumes requiring scaling groups
- **Reliability**: Medium