Blue Team: Summary of Operations

Table of Contents
- Network Topology
- Description of Targets
- Monitoring the Targets
- Patterns of Traffic & Behavior

Network Topology

The following machines were identified on the network:
- Name of VM 1: Hyper-V
  - **Operating System**: Windows
  - **Purpose**: Gateway
  - **IP Address**:192.168.1.1
- Name of VM 2: Kali
  - **Operating System**: Linux
  - **Purpose**: Attacking Machine
  - **IP Address**:192.168.1.90
- Name of VM 3: ELK
  - **Operating System**: Linux
  - **Purpose**: Monitoring/Logging
  - **IP Address**:192.168.1.100
- Name of VM 4: Capstone
  - **Operating System**: Linux
  - **Purpose**: Forwarding Logs
  - **IP Address**:192.168.1.105
- Name of VM 5: Target1
  - **Operating System**: Linux
  - **Purpose**: Target Machine
  - **IP Address**:192.168.1.110
- Name of VM 6: Target2
  - **Operating System**: Linux
  - **Purpose**: Secondary Target Machine
  - **IP Address**:192.168.1.115

Description of Targets

The target of this attack was: 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:

Excessive HTTP Errors could indicate a potential brute force attack on our web server, and as such, we have configured an alert to detect when HTTP error codes are being received at large

Monitoring the Targets

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

These services are vulnerable to potential cross-site-scripting, and HTTP Request Size is an excellent indicator of this attack. Ff an attacker makes a large HTTP Request our alarm will fire

Name of Alert 1
TODO: Replace `Alert 1` with the name of the alert.

Alert 1 is implemented as follows:
- **Metric**: Excessive HTTP Errors
- **Threshold**: >400/5min
- **Vulnerability Mitigated**: Brute Force Attacks
- **Reliability**: This is a high reliability alert, continuous, exorbitant amounts of HTTP Errors is an excellent indicator of a Brute Force Attack, and should always be acknowledged

Name of Alert 2
Alert 2 is implemented as follows:
- **Metric**: HTTP Request Bytes Over All Documents
- **Threshold**: >3500/1min
- **Vulnerability Mitigated**: Cross-Site-Scripting
- **Reliability**: Medium Reliability. There are better methods to prevent attacks of this nature, and there are potential outliers for non-malicious actions being flagged. Should probably still be looked at if alert triggers

Name of Alert 3

Alert 3 is implemented as follows:

- **Metric**: CPU Usage
- **Threshold**: Total CPU Usage >0.5/5min
- **Vulnerability Mitigated**: Malicious Services Running in the Background
- **Reliability**: Low Reliability. Can trigger when unnecessary. Many hackers have adapted to this, and will mask the service as useful, but high usage.