Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- target1
  - **Debian Linux Jessie**:
  - **Wordpress Website**:
  - **192.168.1.110**:
- target2
  - **Debian Linux Jessie**:
  - **Hardened Wordpress Website**:
  - **192.168.1.115**:
- Kali
  - **Kali Linux**
  - **Computer used to do reconnaissance and active breach**
  - **192.168.1.90**
- ELK
  - **Ubuntu 18.04.4 LTS**
  - **Log Management/SIEM/SOC Dashboards**
  - **192.168.1.100**
- Capstone
  - **Ubuntu 18.04.4 LTS**
  - **Test Alerts**
  - **192.168.1.105**

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. Due to this, we have implemented the alerts below:

Excessive HTTP Errors
Alert 1 is implemented as follows:
  - **Metric**: Count of HTTP Status codes above 400
  - **Threshold**: When the number of status codes over 400 are in the top 5 counts of status codes in the prior 5 minutes.
  - **Vulnerability Mitigated**: Brute force / dictionary mapping of a web server
  - **Reliability**: This has a medium reliability as if the majority of traffic is good and receives 200 codes, but someone mistypes a URL. If only the good traffic and the one mis-typed URL are the only traffic in the past 5 minutes the alert would trigger and would be a false positive.

HTTP Request Size Monitor
Alert 2 is implemented as follows:
  - **Metric**: HTTP Request Bytes for the last minute
  - **Threshold**: When HTTP Request Bytes are more than 3500 for the last minute.
  - **Vulnerability Mitigated**: Denial of Service Attacks
  - **Reliability**: This has a high reliability as this is 10 times the normal amount of traffic that is seen on average.

CPU Usage Monitor
Alert 3 is implemented as follows:
  - **Metric**: System Processor Total Usage %
  - **Threshold**: When the system has a total processor usage of over 50%
  - **Vulnerability Mitigated**: Excessive CPU usage due to malware.
  - **Reliability**: This has a medium reliability as updates and/or legitimate high traffic times could trigger an alert.

Suggestions for Going Further (Optional)
The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:
- Vulnerability 1 - **Bruteforce Attack**
  - **Patch**: Install the Wordfence Web Application Firewall via Plugin in Wordpress
  - **Why It Works**: Wordfence has built-in scans and counters to stop erroneous attempts to login/traverse a website.
- Vulnerability 2 - **Denial of Service**
  - **Patch**: Install the Wordfence Web Application Firewall via Plugin in Wordpress
  - **Why It Works**: Wordfence has builtin scans for Denial of Service that can be used to alert and be added to the edge firewall to stop the attacks prior to hitting the web server.
- Vulnerability 3 - **Undetected Malware Activity**

  - **Patch**: Install Network/Machine monitoring via a docker image of Zabbix.
  - **Why It Works**: Zabbix monitors and reports abou odd conditions on a network or server ranging for CPU usage to increases in network traffic.