Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Capstone
  - **Operating System**: Ubuntu 18.01.1 LTS
  - **Purpose**: Web server that handles the http requests and web resources.
  - **IP Address**: 192.168.1.105
- ELK
  - **Operating System**: Linux
  - **Purpose**: Monitors and collects Logs, provides network analytics.
  - **IP Address**: 192.168.1.100
- Kali
  - **Operating System**: Kali Linux
  - **Purpose**: System used for network scanning, pentesting, and security auditing.
  - **IP Address**: 192.168.1.90
- Target 1
  - **Operating System**: Debian Linux 3.2-4.9
  - **Purpose**: Main target virtual machine we will be trying to exploit
  - **IP Address**: 192.168.1.110
- Target 2
  - **Operating System**: Linux 3.2-4.9
  - **Purpose**: Secondary target virtual machine we will be trying to exploit
  - **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:

Alert 1: *HTTP Request Size Monitor*

Alert 1 is implemented as follows:

- **Metric**: http.request.bytes
- **Threshold**: over 3500 over last 60 seconds
- **Vulnerability Mitigated**: http POST Vulnerability
- **Reliability**: High Reliability

Alet 2: *Excessive HTTP Errors*

Alert 2 is implemented as follows:

- **Metric**: http.response.status_code
- **Threshold**: above 40 over 5 minutes
- **Vulnerability Mitigated**: Brute-Force Login Attempt
- **Reliability**: High Reliability

Alert 3: CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: system.process.cpu.total.pct
- **Threshold**: above .5
- **Vulnerability Mitigated**: Denial of Service
- **Reliability**: High Reliability. A couple of false positives triggered but only two.

Suggestions for Going Further

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: **HTTP POST Request Vulnerability**
    - **Patch**: Implement controls restricting POST requests to the server.
    - **Why It Works**: Restricting http POST ability to known sources only would mitigate risks of malicious file payloads and code injections.
- Vulnerability 2: **Brute Force Login**
    - **Patch**: Configure failed password control protocol to restrict the number of failed logins.

    - **Why It Works**: By temporarily locking accounts due to failed logins, the server is much less vulnerable to a brute force login attack.
- Vulnerability 3: **Denial of Service**
    - **Patch**: Utilize an Intrusion Prevention System (IPS).
    - **Why It Works**: This provides an extra layer of security by restricting traffic based on rules to ensure legitimate traffic into your network while also prioritizing system resources.