Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Kali
    - Operating System: Linux
    - Purpose: Attacker Machine
    - IP Address: 192.168.1.90
- ELK
    - Operating System: Linux
    - Purpose: Elasticsearch, Logstash, Kibana Server; holds Kibana dashboards
    - IP Address: 192.168.1.100
- Capstone
    - Operating System: Linux
    - Purpose: Testing Alerts
    - IP Address: 192.168.1.105
- Target 1
    - Operating System: Linux
    - Purpose: Exposes a vulnerable WordPress server
    - IP Address: 192.168.1.110

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: Excessive HTTP Errors, HTTP Request Size Monitor, and CPU Usage Monitor.

Monitoring the Targets

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

Alert 1: Excessive HTTP Errors

Alert 1 is implemented as follows:

- **Metric**: packetbeat
- **Threshold**: 400 in 5 minutes
- **Vulnerability Mitigated**: Attacks can be identified so the IP addresses can be blocked, password changes, or port 22 can be closed or filtered
- **Reliability**: This alert does not generate a lot of false positives and has a high reliability rate

Alert 2: HTTP Request Size Monitor

Alert 2 is implemented as follows:

- **Metric**: packetbeat
- **Threshold**: 3,500 in 1 minute
- **Vulnerability Mitigated**: DDOS attacks are mitigated by controlling the number of HTTP requests
- **Reliability**: This alert is reliable and does not create a lot of false positives

Alert 3: CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: metricbeat
- **Threshold**: .5 in 5 minutes
- **Vulnerability Mitigated**: By keeping the CPU usage to 50%, a memory dump will be triggered when the threshold is reached
- **Reliability**: This alert can trigger a lot of false positives because the CPU can spike even if there is not attack

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 - Excessive HTTP Requests
    - **Patch**: Use a stronger password policy

    - **Why It Works**: Stronger passwords are tougher to brute force
- Vulnerability 2 - HTTP Request Size Monitor
    - **Patch**: Use multi-layer defense such as firewalls, VPN, load balancing, etc.
    - **Why It Works**: Having a secure infrastructure can minimize the threat of DDOS attacks
- Vulnerability 3 - CPU Usage Monitor
    - **Patch**: Use Host-based IPS (Intrusion Prevention System) to prevent a DDOS attack
    - **Why It Works**: Malware is stopped by monitoring the behavior of the code