Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Kali
    - **Operating System**: Kali Linux
    - **Purpose**: Attacking Machine
    - **IP Address**: 192.168.1.90
- Target 1
    - **Operating System**:
    - **Purpose**: Vulnerable WordPress Server
    - **IP Address**: 192.168.1.110
- Capstone
    - **Operating System:** Linux
    - **Purpose:** Forward Logs to ELK Machine
    - **IP Address:** 192.168.1.105
- ELK
    - **Operating System:** Linux
    - **Purpose:**
    - **IP Address:** 192.168.1.100

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:

HTTP Request Size Monitor

- **Metric**: WHEN sum() OF http.request.bytes OVER all documents is ABOVE 3500 FOR THE LAST 1 minute
- **Threshold**: 3500
- **Vulnerability Mitigated**: Code Injection in HTTP Requests
- **Reliability**: Medium reliability, this alert could trigger some false positives as there could be large authentic HTTP requests or HTTP traffic

Excessive HTTP Errors

- **Metric**: WHEN count() GROUPED OVER top 5 ‘http.response.status_code’ IS ABOVE 400 FOR THE LAST 5 minutes
- **Threshold**: 400
- **Vulnerability Mitigated**: Brute Force Vulnerability
- **Reliability**: High reliability as this alert will only trigger when a response code of 400 is sent out, filtering out any successful response codes.

CPU Usage Monitor

- **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Threshold**: 0.5
- **Vulnerability Mitigated**: Malicious Programs/Malware
- **Reliability**: Highly reliable, even if there isn't malware running or a malicious program running, this alert could help to improve CPU usage

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
    - Patch: Disable SSH
        - This can be done by editing the /etc/ssh/sshd_config file and removing non root SSH access
    - Why It Works: disabling SSH for non root users mitigates against regular users machines becoming infected and used as a gateway into the web server or system
- Vulnerability 2
    - Patch: Implement Stronger Password Policies
        - Enforce users to use special characters along with upper and lower case letters
        - Enforce password history
        - Multi-Factor Authentication
        - Do not use personal information
    - Why It Works: Complex password take longer to brute force turning attackers away from trying to brute force their way in
- Vulnerability 3
    - Patch: Configure and hash Wordpress database login information
        - Hashing the password for the wordpress database ensures that even if the config file is accessed, the password is not written in plaintext
    - Why It Works: Encrypting sensitive data such as passwords to the MySQL database make it harder to an attacker to gain more sensitive information that could do more damages
- Vulnerability 4
    - Patch: Configure user privileges and file permissions
        - Set correct file permissions for user accounts; general users should not have access to Wordpress configuration file
        - General users should not have access to use python commands unless required for their role
    - Why It Works: Correct file and user permissions mitigate against those users potentially becoming compromised and used as gateways to perform more damaging attacks