Blue Team: Summary of Operations

Table of Contents

Network Topology

TODO: Fill out the information below.

The following machines were identified on the network:

- Name of VM 1
    - **Operating System**: Debian GNU/Linux
    - **Purpose**: Target 1
    - **IP Address**: 192.168.1.110
- Name of VM 2
    - **Operating System**: Debian GNU/Linux
    - **Purpose**: Target 2
    - **IP Address**: 192.168.1.115

Description of Targets

TODO: Answer the questions below.

The target of this attack was: Target 1 (TODO: 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:

Name of Alert 1

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

Alert 1 is implemented as follows:

- **Metric**: HTTP errors
- **Threshold**: above 400 for the last 5mins
- **Vulnerability Mitigated**: Brute force attack. Resource usage issues
- **Reliability**: High reliability.

Name of Alert 2

Alert 2 is implemented as follows:

- **Metric**: http.request.bites
- **Threshold**: aove 3500 for the last minute
- **Vulnerability Mitigated**: DOS attack
- **Reliability**: High reliability.

Name of Alert 3

Alert 3 is implemented as follows:

- **Metric**: system.process.cpu.total.pct
- **Threshold**: above 0.5for the last 5mins
- **Vulnerability Mitigated**: Resource management
- **Reliability**: High reliability.

TODO Note: Explain at least 3 alerts. Add more if time allows.

Suggestions for Going Further (Optional)

TODO:

- Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain *how* to implement each patch.

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 Brute force attack
- **Patch**: invalid credential will eventually lock out
- **Why It Works**: only trusted ip addresses will be allowed access

- Vulnerability 2 DOS attack
    - **Patch**: load balancer installation is highly advised
    - **Why It Works**:

Vulnerability 3. Excessive CPU Usage

- **Patch**: each core must have a limit cpu usage
- **Why It Works**: Good management of power cords