Blue Team: Summary of Operations

Table of Contents

- Network Topology
- Description of Targets
- Monitoring the Targets
- Patterns of Traffic & Behavior
- Suggestions for Going Further

Network Topology

The following machines were identified on the network:

- Kali
 - Kali GNU/Linux Rolling
 - Attacking machine
 - 0 192.168.1.110
- Target 1
 - Debian GNU/Linux 8
 - Target Machine
 - 0 192.168.1.110
- ELK
 - o Ubuntu 18.04.4
 - Network Monitor
 - 0 192.168.1.100
- Target 2
 - Debian GNU/Linux 8 (jessie)
 - Target Machine
 - 0 192.168.1.115
- Capstone
 - o Ubuntu 18.04
 - o The Vulnerable Web Server
 - o 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:

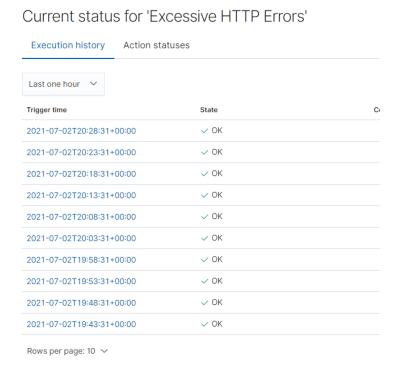
Monitoring the Targets

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

Excessive HTTP Errors

WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes

- Metric: When one of the top 5 HTTP response codes is in the 400s, indicating an error.
- Threshold: 400
- Vulnerability Mitigated: Would alert you to a Brute Force when you have many repeated HTTP errors
- **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.



HTTP Request Size Monitor

- Metric: When the total request size over the whole system is over 3500 bytes in 1 minute.
- Threshold: 3500 bytes
- Vulnerability Mitigated: Malicious Code Injection that could cause XSS(Cross Site Scripting) or DDoS attacks
- **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

Execution history Action statuses Last one hour ~ Trigger time State 2021-07-02T20:28:31+00:00 ✓ OK ✓ OK 2021-07-02T20:23:31+00:00 2021-07-02T20:18:31+00:00 ✓ OK 2021-07-02T20:13:31+00:00 \checkmark OK 2021-07-02T20:08:31+00:00 ✓ OK 2021-07-02T20:03:31+00:00 ✓ OK 2021-07-02T19:58:31+00:00 ✓ OK 2021-07-02T19:53:31+00:00 ✓ OK ✓ OK 2021-07-02T19:48:31+00:00 ✓ OK 2021-07-02T19:43:31+00:00 Rows per page: 10 ∨

Current status for 'CPU Usage Monitor'

CPU Usage Monitor

₩EN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

- Metric: When the total CPU usage percentage goes over 0.5% over the last 5 minutes
- Threshold: 0.5%
- Vulnerability Mitigated: Cryptojacking and other malicious programs live viruses and malware that take up CPU resources
- **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

Current status for 'HTTP Request Size Monitor'

Execution history	Action statuses		
Last one hour ~			
Trigger time		State	
2021-07-02T20:30:31+00:00		✓ OK	
2021-07-02T20:29:31+00:00		✓ OK	
2021-07-02T20:28:31+	00:00	✓ OK	
2021-07-02T20:27:31+00:00		✓ OK	
2021-07-02T20:26:31+	00:00	✓ OK	
2021-07-02T20:25:31+00:00		✓ OK	
2021-07-02T20:24:31+00:00		✓ OK	
2021-07-02T20:23:31+00:00		✓ OK	
2021-07-02T20:22:32+00:00		✓ OK	
2021-07-02T20:21:31+00:00		✓ OK	

Rows per page: 10 ∨