

Blue Team: Summary of Operations

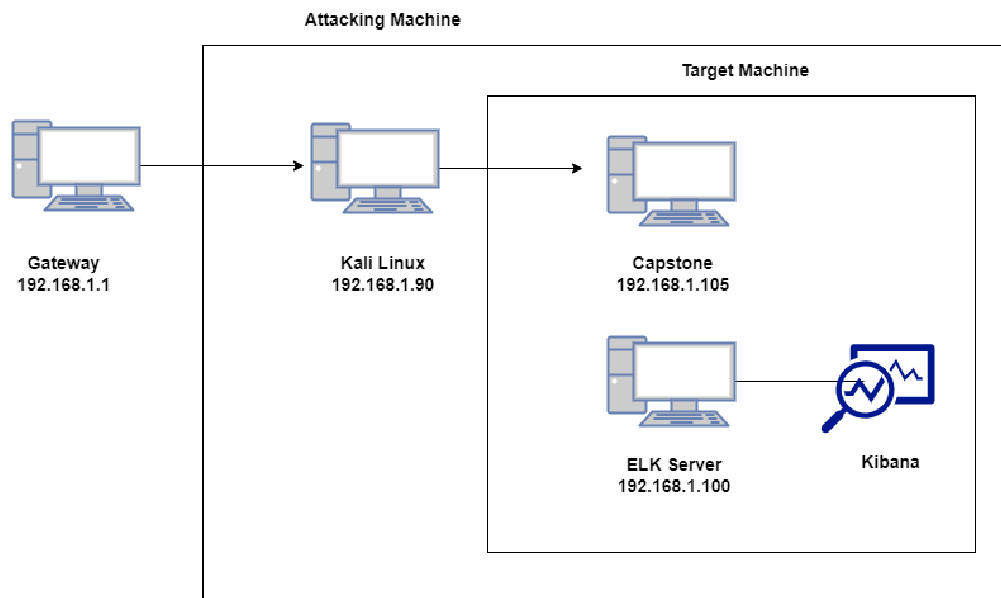
Table of Contents

- Network Topology
- Description of Targets
- Monitoring the Targets
- Patterns of Traffic & Behavior

Network Topology

The following machines were identified on the network:

- **Gateway**
 - Windows 10 Pro
 - Starting point/entry point
 - 192.168.1.1
- **ELK Server**
 - Linux
 - Used for Kibana
 - 192.168.1.100
- **Capstone**
 - Linux
 - The machine being targeted
 - 192.168.1.105
- **Kali Linux**
 - Linux
 - Used for penetration testing
 - 192.168.1.90



Description of Targets

The target of this attack was: **192.168.1.105**

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:

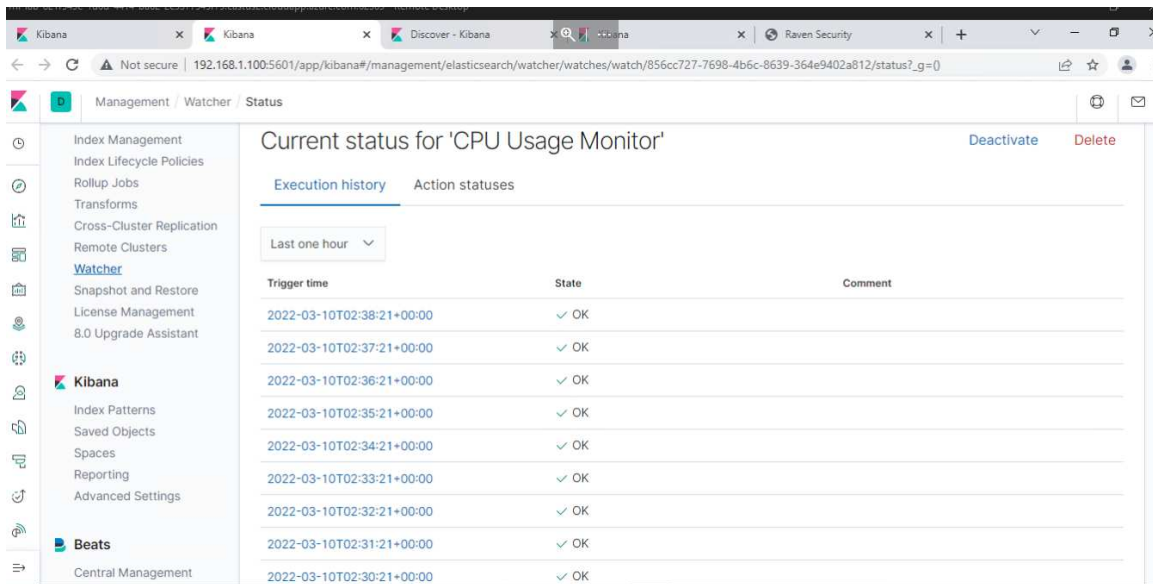
Monitoring the Targets

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

-CPU Usage Monitor

Alert 1 is implemented as follows:

- Metric: WHEN mac() OF system.process.cpu.pct OVER all documents
- Threshold: IS ABOVE 0.5 FOR THE LAST 5 minutes
- Vulnerability Mitigated: Checks what is using the CPU
- Reliability: High



The screenshot shows the Kibana Watcher interface in a web browser. The URL bar indicates the path to the 'CPU Usage Monitor' watch status. The left sidebar contains navigation links for various Kibana features. The main content area displays the 'Current status for 'CPU Usage Monitor'' with tabs for 'Execution history' and 'Action statuses'. The 'Execution history' tab is active, showing a table of recent executions with columns for 'Trigger time', 'State', and 'Comment'. All listed executions show a state of 'OK'.

Trigger time	State	Comment
2022-03-10T02:38:21+00:00	✓ OK	
2022-03-10T02:37:21+00:00	✓ OK	
2022-03-10T02:36:21+00:00	✓ OK	
2022-03-10T02:35:21+00:00	✓ OK	
2022-03-10T02:34:21+00:00	✓ OK	
2022-03-10T02:33:21+00:00	✓ OK	
2022-03-10T02:32:21+00:00	✓ OK	
2022-03-10T02:31:21+00:00	✓ OK	
2022-03-10T02:30:21+00:00	✓ OK	

-HTTP Request Size Monitor

Alert 2 is implemented as follows:

- Metric: WHEN sum() of http.request OVER all documents
- Threshold: IS ABOVE 3500 FOR THE LAST 1 minute
- Vulnerability Mitigated: Checks for webpage availability (HTTP requests)
- Reliability: Medium

Management / Watcher / Status

Current status for 'HTTP Request Size Monitor'

Deactivate Delete

Execution history Action statuses

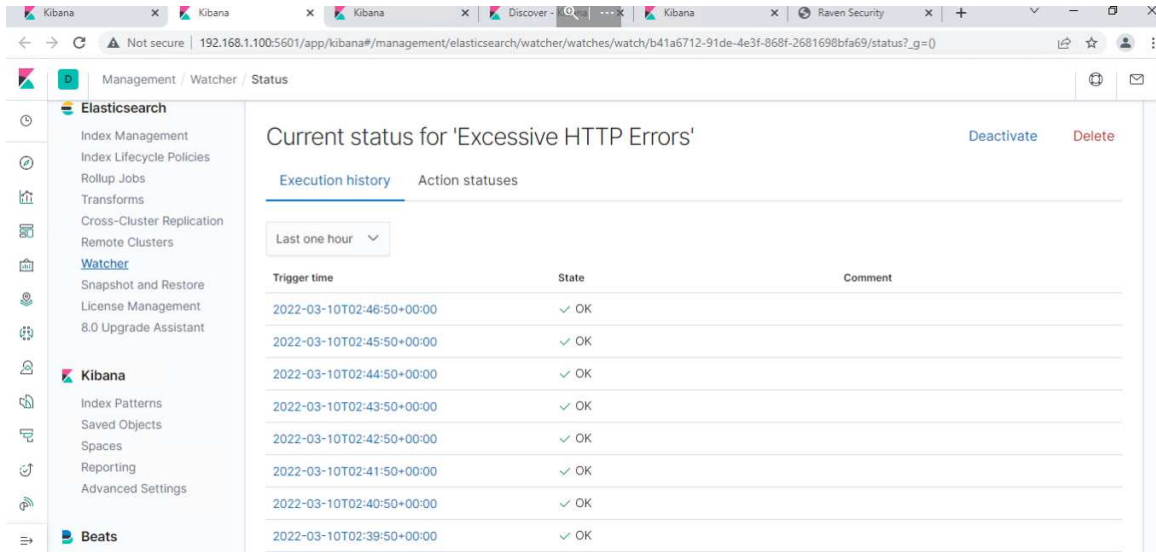
Last one hour

Trigger time	State	Comment
2022-03-10T02:47:24+00:00	Firing	
2022-03-10T02:46:24+00:00	Firing	
2022-03-10T02:45:24+00:00	Firing	
2022-03-10T02:44:24+00:00	Firing	
2022-03-10T02:43:24+00:00	Firing	
2022-03-10T02:42:24+00:00	Firing	
2022-03-10T02:41:24+00:00	Firing	
2022-03-10T02:40:24+00:00	Firing	
2022-03-10T02:39:24+00:00	Firing	

-Excessive HTTP Errors

Alert 3 is implemented as follows:

- Metric: When count() GROUPED OVER top 5 'http.response.status_code'
- Threshold: IS ABOVE 400 FOR THE LAST 5 minutes
- Vulnerability Mitigated: Enumeration
- Reliability: High



Management / Watcher / Status

Current status for 'Excessive HTTP Errors'

[Deactivate](#) [Delete](#)

[Execution history](#) [Action statuses](#)

Last one hour

Trigger time	State	Comment
2022-03-10T02:46:50+00:00	✓ OK	
2022-03-10T02:45:50+00:00	✓ OK	
2022-03-10T02:44:50+00:00	✓ OK	
2022-03-10T02:43:50+00:00	✓ OK	
2022-03-10T02:42:50+00:00	✓ OK	
2022-03-10T02:41:50+00:00	✓ OK	
2022-03-10T02:40:50+00:00	✓ OK	
2022-03-10T02:39:50+00:00	✓ OK	