**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:

|  |  |
| --- | --- |
| VM Kali  Operating System: Linux  Purpose: Attacker  IP Address: 192.168.1.90 | Raven Target1  Operating System: Linux Debian  Purpose: First attack target Apache Web Server  IP Address: 192.168.1.110 |
| Raven Target2  Operating System: Linux Debian  Purpose: Second attack target Apache Web Server  IP Address: 192.168.1.115 | ELK Stack  Operating System: Linux Ubuntu  Purpose: ELK Stack Server  IP Address: 192.168.1.100 |
| ML-RefVm-684427  Operating System: Windows  Purpose: VM Host  IP Address: 192.168.1.1 | Capstone  Operating System: Linux Purpose: Apache Webserver  IP Address: 192.168.1.105 |

**Description of Targets**

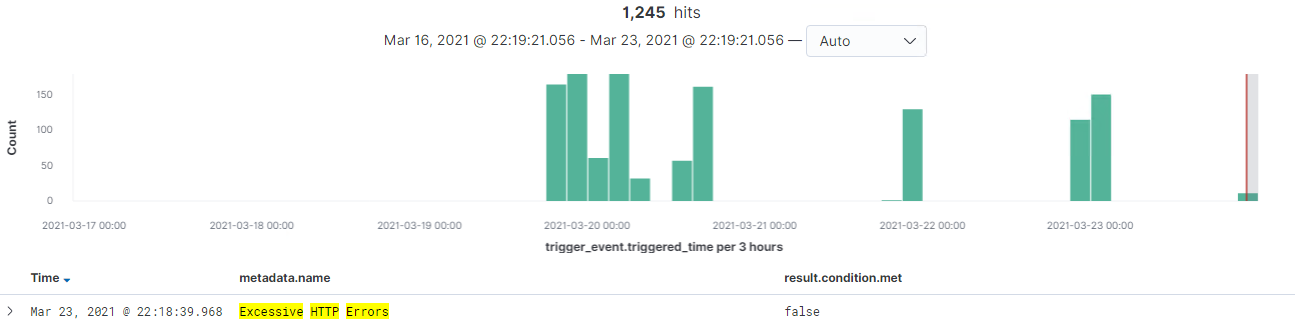
Target IP Address 192.168.1.110

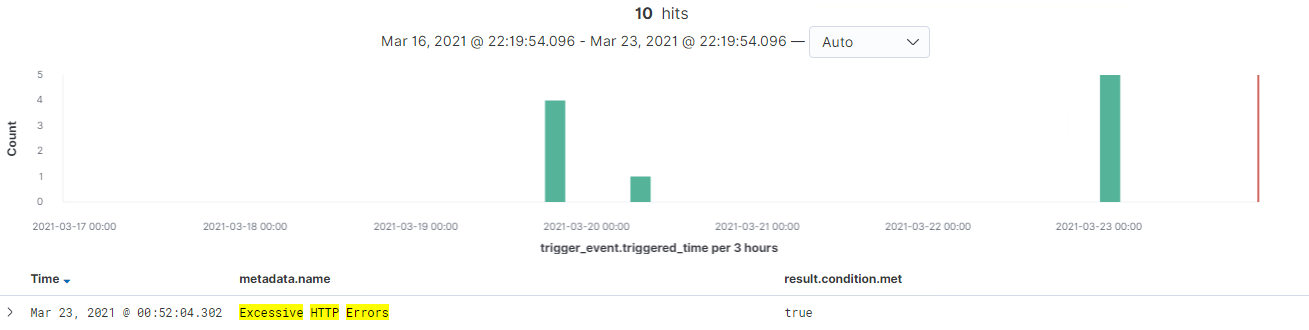
Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

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

**Excessive HTTP Errors**

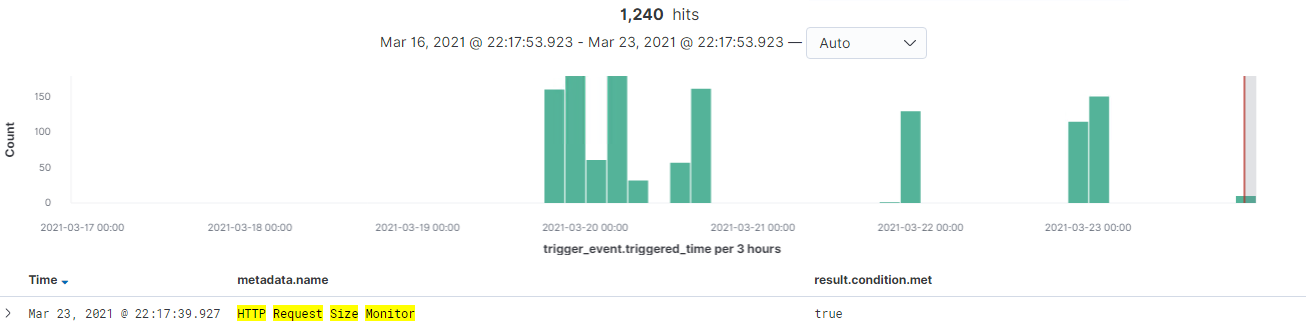
|  |  |
| --- | --- |
| Excessive HTTP errors is implemented as follows: | |
| **Metric:** | http.response.status\_code |
| **Threshold:** | HTTP RESPONSES are above 400 for the last 5 minutes |
| **Vulnerability Mitigated:** | CVE-2018-1312, CVE 2019-0217, 2019-0211, CVE-2015-5600 |
| **Reliability:** | High |
| **Rationale:** | The alert indicated that of 1,245 watched events only 10 matched the alert criteria. The events that triggered the alert was Brute forcing attack to gain access through a user’s account. |
| **Patch:** | To resolve this issue there are numerous steps that can be taken to remedy. For example, switch from password authentication to public key authentication, or even disabling SSH all together. |
| **Why it Works:** | Disabling SSH would in turn mean that no one could access the server from outside the firewall. Another alternative would be to turn off password authentication and instead have it set to authenticate based on public keys. This concept can be spread across the network through an ansible playbook. |

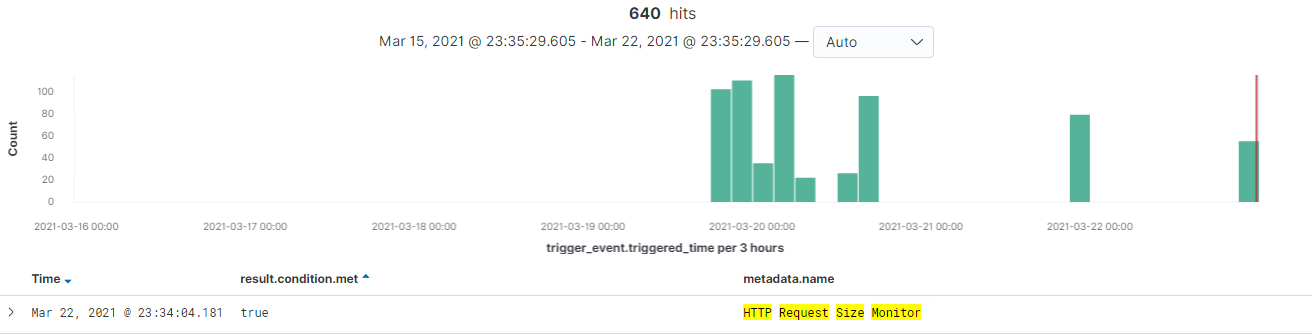




**HTTP Request Size**

|  |  |
| --- | --- |
| HTTP Request Size is implemented as follows | |
| **Metric:** | http.request.bytes |
| **Threshold:** | HTTP Request Sizes above 3500 Bytes in 1 minute |
| **Vulnerability Mitigated:** | CWE-548 |
| **Reliability:** | LOW |
| **Rationale:** | The alert generates a lot of false positives because the request can vary based on the type of HTTP request sent. Various actions trigger the alert; for example, saving a html link, and even scanning such as a WP Scan against the system. |
| **Patch:** | * Increase the HTTP request size * Restrict the HTTP requests to just POST requests |
| **Why it Works:** | * Request sizes vary significantly today * no user should be allowed to upload to the system/site. |





**CPU Usage Monitor**

|  |  |
| --- | --- |
| CPU Usage Monitor | |
| **Metric:** | system.process.cpu.total.pct |
| **Threshold:** | CPU Processes is above 50% for last 5 minutes |
| **Vulnerability Mitigated:** | CVE-2018-1303 |
| **Reliability:** | HIGH |
| **Rationale:** | There were 32 hits that fit the alert criteria out of 1236 results. |
| **Patch:** | The activities that could cause CPU Usage to increase include brute force attacks, attacks on Apache, Network attacks, and even a special crafted HTTP request header that exceeds the bounds set to aid in causing a denial of service .   * A patch that would reduce the chances of a CPU Usage being wasted would be to alter the Limit directives. For example, The Limit RequestBody, RequestFeilds, RequestFeildSize, should be carefully configured. * Install mod\_evasive to provide evasive action in the event of an HTTP DOS or DDOS. |
| **Why it Works:** | * By limiting the resource consumption triggered by client input there is less opportunity for external impact on internal services. * Mod evasive is an evasive maneuvers module for Apache. It provides evasive action in the event of HTTP DOS or DDOS attacks or Brute force attacks. |

