Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Kali
  - **Operating System**: Linux
  - **Purpose**: Attacker
  - **IP Address**:192.168.1.90
- ELK
  - **Operating System**: Linux
  - **Purpose**: Observation with kibana
  - **IP Address**:192.168.1.100
- Capstone
  - **OS**: Linux
  - **Purpose**: Alerting/ Sending logs
  - **IP Address**: 192.168.1.105
- Target1
  - **OS**: Linux
  - **Purpose**: Target
  - **IP Address**: 192.168.1.110

Description of Targets

The target of this attack was: Target 1- 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:

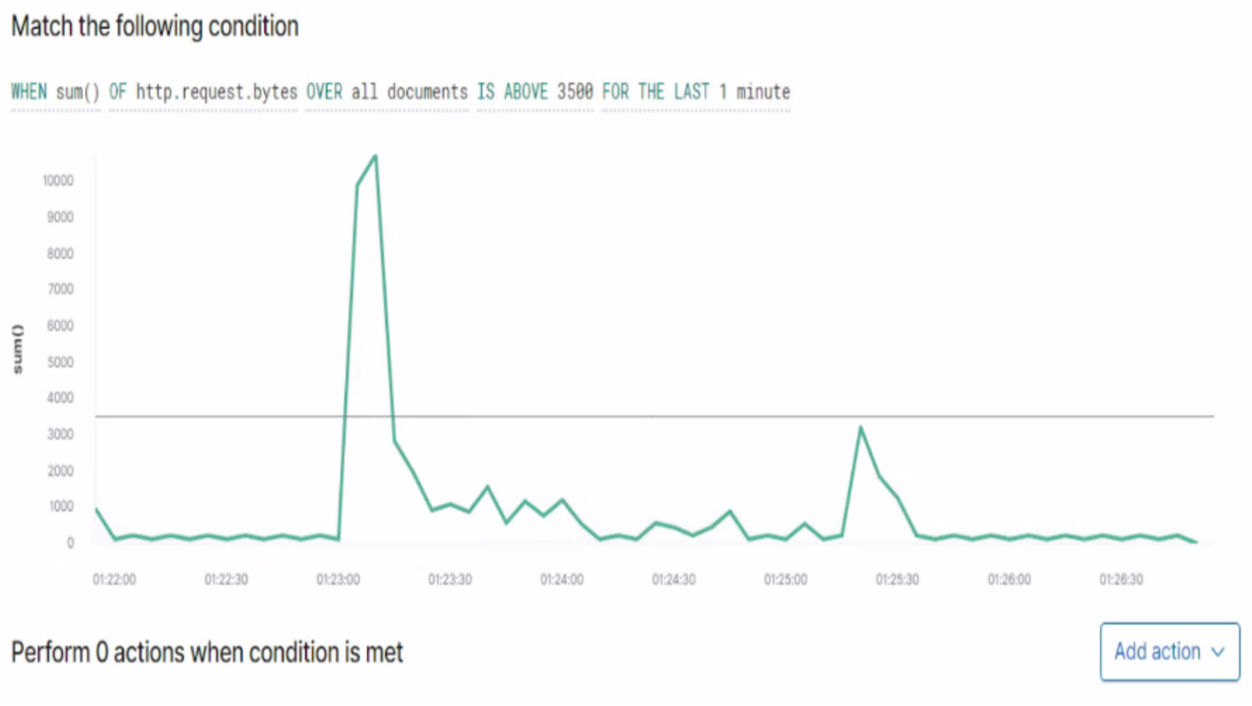
Monitoring the Targets

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

Excessive HTTP Errors

Alert 1 is implemented as follows:

- **Metric**: when sum of http.request.bytes over all documents
  - Packets from same IP to all destination ports
- **Threshold**: above 3500 for the last 1 minute
- **Vulnerability Mitigated**: Network/Port scan
- **Reliability**: medium reliability due to the fact that one spike was under the threshold and created a false negative



Match the following condition

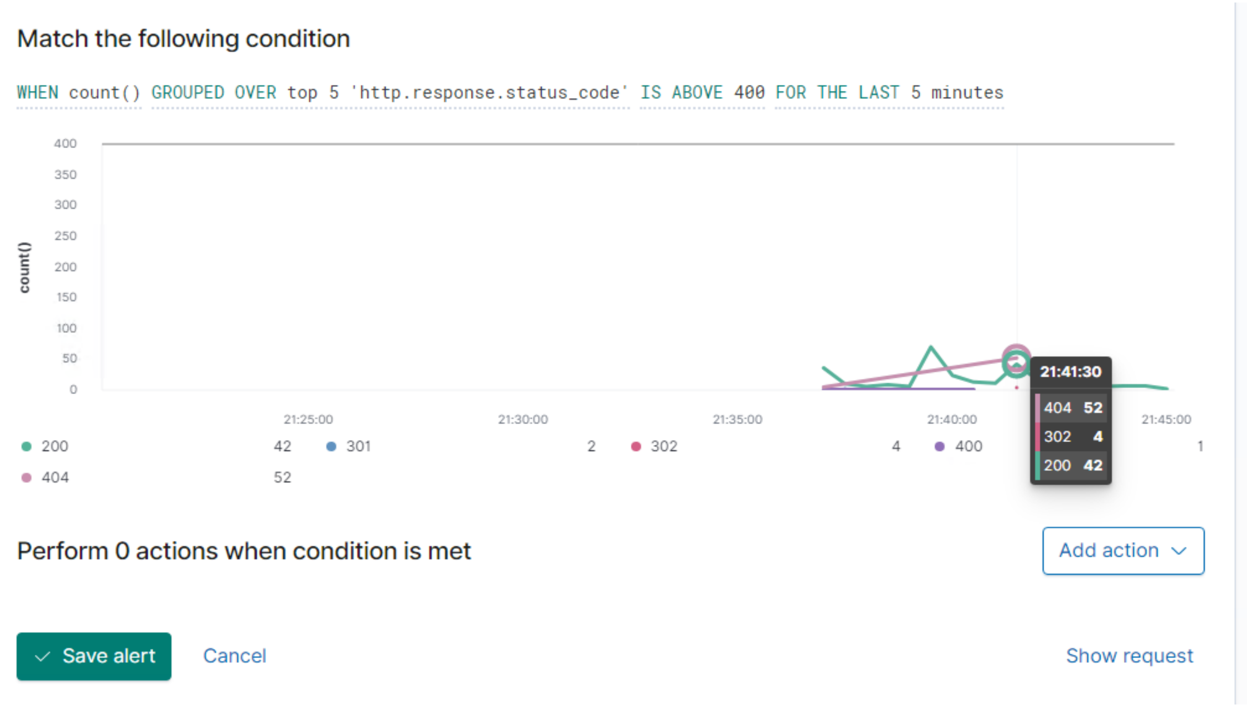
```
WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
```

Perform 0 actions when condition is met

HTTP Request Size Monitor

Alert 2 is implemented as follows:

- **Metric**: when count grouped over top 5 ‘http.response.status.code’
  - packets attempting to access network resources
- **Threshold**: above 400 for the last 5 minutes
- **Vulnerability Mitigated**: Wordpress enumeration
- **Reliability**: low reliability since it only reached 52 “404” responses, not triggering it at that very high 400 alert



Match the following condition

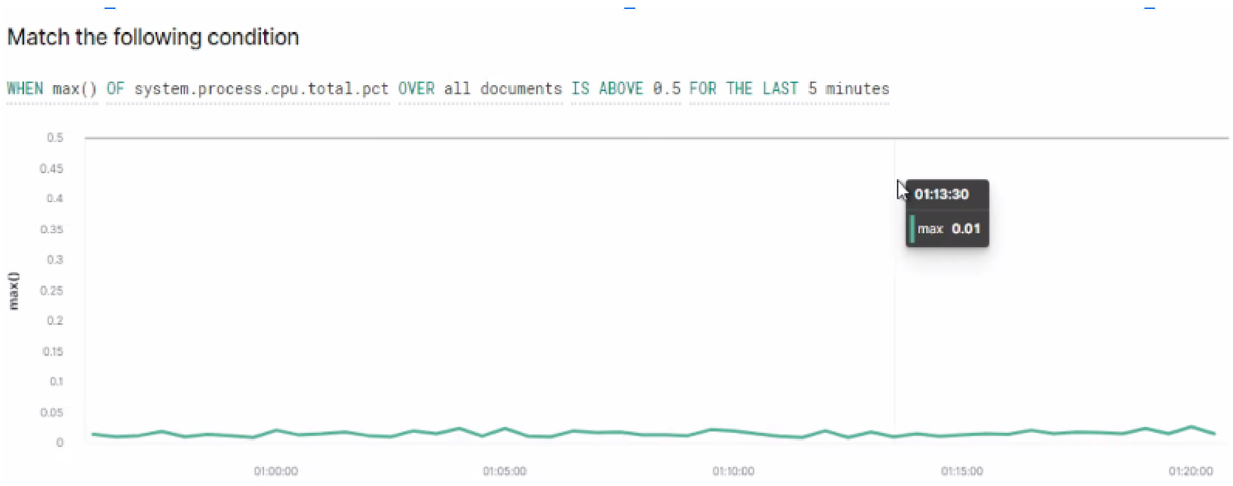
```
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
```

Perform 0 actions when condition is met

CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: when max of system.process.cpu.total.pct over all documents
  - system CPU processes
- **Threshold**: above .5 for the last 5 minutes
- **Vulnerability Mitigated**: Password cracking
- **Reliability**: low reliability since the passwords hashes were cracked outside the users machine and did not trigger an alert



Match the following condition

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

Suggestions for Going Further (Optional)

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:network/port scan
    - **Patch**: Cyber Threat Intelligence (CTI), properly installed firewall with updated applications, closed ports, TCP wrappers,
    - **Why It Works**: CTI works by collecting data and processing it throughout history to prevent “like” attacks from happening. It studies who or what is attacking, why they are choosing the target and how to spot signs of compromise. A firewall is able to detect the sccan and shut it down. A TCP wrapper gives admins control over what IP address can have access to the network.

(*What Is Cyber Threat Intelligence?*, n.d.)

- Vulnerability 2: wordpress enumeration
    - **Patch**: add the following code to the functions.php file

      ```
      // block WP enum scans
      // https://m0n.co/enum
      if (!is_admin()) {
              // default URL format
              if (preg_match('/author=([0-9]*)/i',$_SERVER['QUERY_STRING'])) die();
              add_filter('redirect_canonical', 'shapeSpace_check_enum', 10, 2);}
      function shapeSpace_check_enum($redirect, $request) {
              // permalink URL format
              if (preg_match('/\?author=([0-9]*)(\/*)/i', $request)) die();
              else return $redirect;}
      ```

    - **Why It Works**: This patch will check if the request is for any page in the WP Admin Area and block the request if it is for a query-string author archive.
    - **Other Patches**: block request at the server level by adding code to the root.htaccess file, change all user display names to anything other than the login name, make sure author tags are not displaying login names

(Starr, 2018)

- Vulnerability 3: Brute Force/ password cracking
    - **Patch**: Strict password policies including MFA, long/complex passwords, different passwords for all accounts, and the use of passphrases
    - **Why It Works**: Making a complex password/ passphrase will avoid the cracking software detecting the correct combination used to log in. MFA will just add another layer of defense that the attacker would need to penetrate.

References

Starr, J. (2018, August 3). *Stop User Enumeration in WordPress*. Perishable Press. Retrieved August 22, 2022, from https://perishablepress.com/stop-user-enumeration-wordpress/

What Is Cyber Threat Intelligence? (n.d.). Fortinet. Retrieved August 22, 2022, from https://www.fortinet.com/resources/cyberglossary/cyber-threat-intelligence