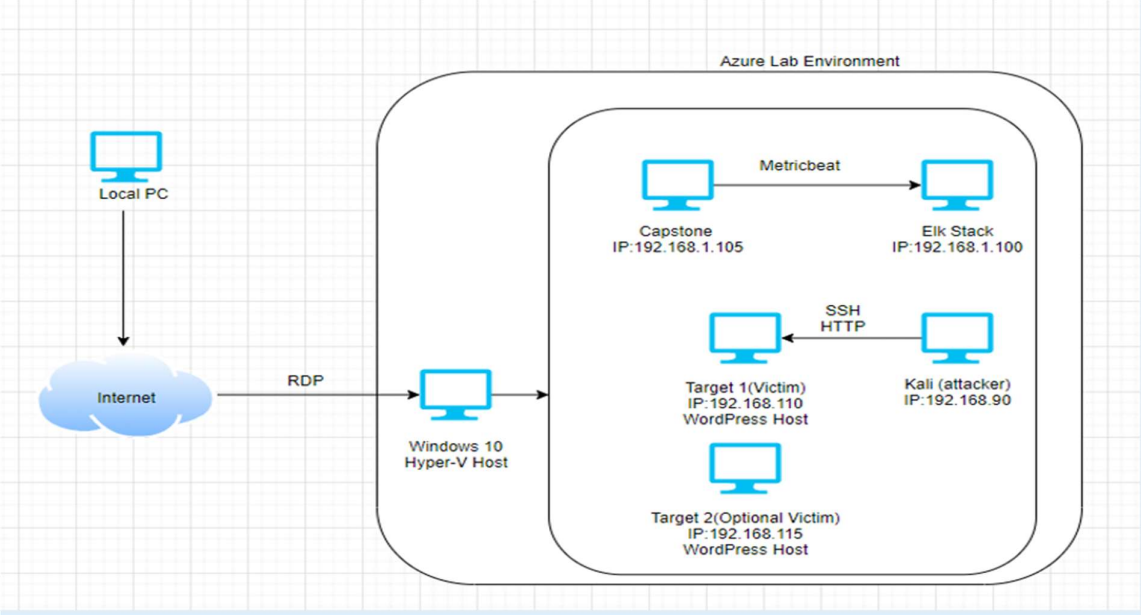
Blue Team: Summary of Operations

Table of Contents

Network Topology



The following machines were identified on the network:

Hyper-V Machine

- Operating System: Windows 10
- Purpose: Host Machine / Gateway
- IP Address: 192.168.1.1

ELK Machine

- Operating System: Ubuntu 18.04
- Purpose: ELK (Elasticsearch & Kibana) Stack
- IP Address: 192.168.1.100

Capstone

- Operating System: Ubuntu 18.04
- Purpose: Capstone contains Filebeat, Metricbeat & Packetbeat that forward logs to ELK Machine
- IP Address: 192.168.1.105

Target 1

- Operating System: Linux 3.2 – 4.9
- Purpose: Vulnerable VM on WordPress server (Target Machine)
- IP Address: 192.168.1.110

Target 2

- Operating System: Linux 3.2 – 4.9
- Purpose: VM with Vulnerabilities (Target Machine)
- IP Address: 192.168.1.115

Kali

- Operating System: Linux 2.6.32
- Purpose: Penetration Test / Attacker Machine
- IP Address: 192.168.1.90

Description of Targets

The target of this attack was: `Target 1` (192.168.1.110) & Target 2` (192.168.1.115 - optional)

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:

- Excessive HTTP Errors
- HTTP Request Size Monitor
- CPU Usage Monitor

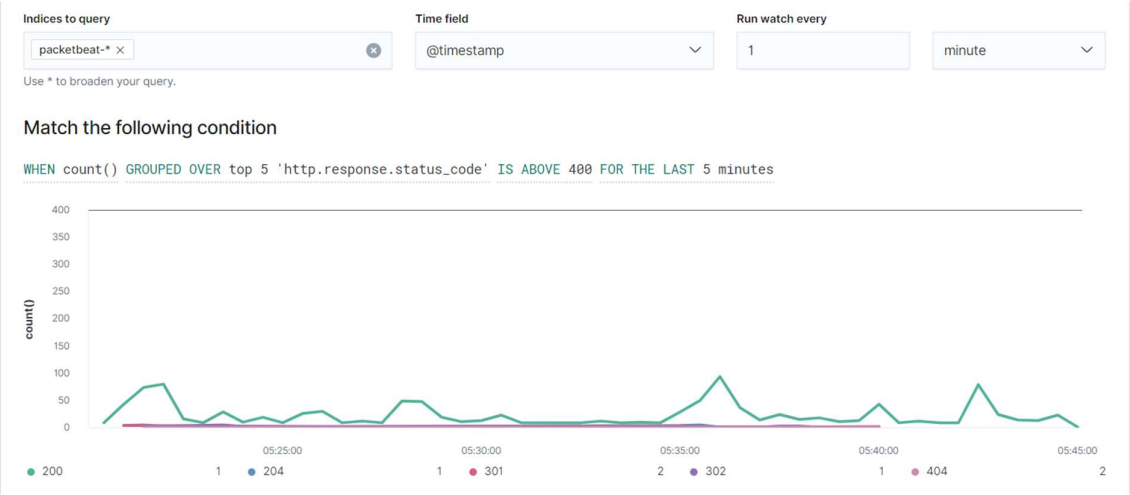
Monitoring the Targets

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

Alert 1 - Excessive HTTP Errors

Excessive HTTP Error is implemented as follows:

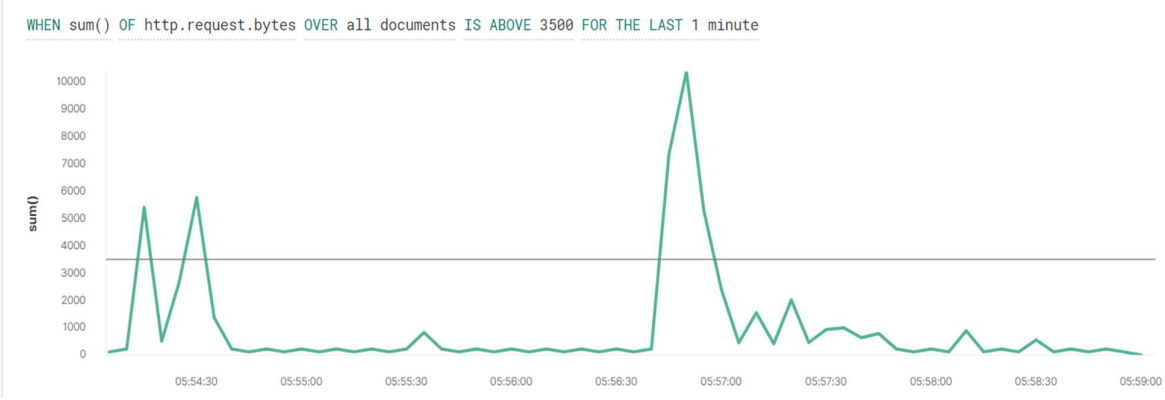
- **Metric:** WHEN count() GROUPED OVER top 5 'http.response.status_code'
- **Threshold:** IS ABOVE 400 FOR THE LAST 5 minutes
- **Vulnerability Mitigated:** By creating alert, security team can identify attacks and control it by blocking ip address, password change and closing port 22
- **Reliability:** The alert is reliable even though it might show some false positives. Measuring by error codes 400 and above will filter out any normal or successful responses. 400+ codes are client and server errors which are of more concern. Especially when considering these error codes going off at a higher rate.



Alert - 2 HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

- **Metric:** WHEN sum() of http.request.bytes OVER all documents
- **Threshold:** IS ABOVE 3500 FOR THE LAST 1 minute
- **Vulnerability Mitigated:** Controlling the number of http request size helps in protecting DDOS attacks
- **Reliability:** Alert could create false positives. Reliability is medium. There is a possibility for a large non malicious HTTP request or legitimate HTTP traffic.

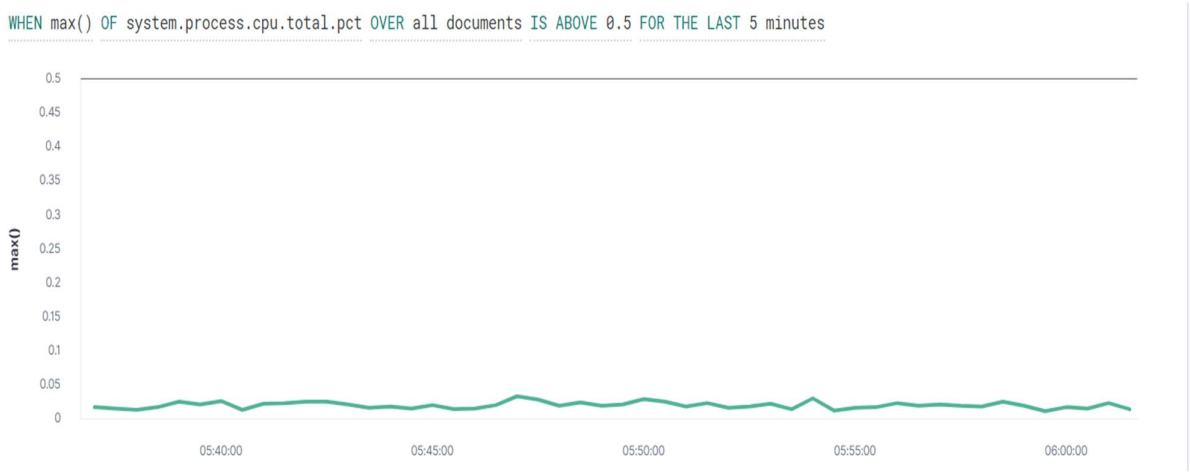


Alert - 3 CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- **Metric:** WHEN max () OF system.process.cpu.total.pct OVER all documents
- **Threshold:** IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Vulnerability Mitigated:** Control on CPU usage helps in identifying malicious programs (malware or viruses) running taking up the resource

- **Reliability:** The alert is highly reliable. Even if there isn't a malicious program running this can still help determine where to improve on CPU usage.



Suggestions for Going Further (Optional)

- Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behaviour, 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.
- 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 - Excessive HTTP Errors

- **Patch: WordPress Hardening**
    - **I**mplement regular updates to WordPress
    - WordPress Core
    - PHP version
    - Plugins
- **Install security plugin(s)**
    - Wordfence (adds security functionality)
- **Disable unused WordPress features and settings like:**
    - WordPress XML-RPC (active by default)
    - WordPress REST API (active by default)
- **Block requests to /?author= by configuring web server settings**
- **Remove WordPress logins from being publicly accessible specifically:**
    - /wp-admin
    - /wp-login.php
- **Why It Works:**
    - Regular updates to WordPress, the PHP version and plugins is an easy way to implement patches or fixes to exploits/vulnerabilities.
    - Depending on the WordPress security plugin it can provide things like:

        - Malware scans
        - Firewall
    - IP options (to monitor/block suspicious traffic)
    - REST API is used by WPScan to enumerate users
        - Disabling it will help mitigate WPScan or enumeration in general
    - XML-RPC uses HTTP as it's method of data transport
    - WordPress links (permalinks) can include authors (users)
        - Blocking request to view the all authors (users) helps mitigate against user enumeration attacks
    - Removal of public access to WordPress login helps reduce the attack surface

Vulnerability – 2 HTTP Request Size Monitor

- **Patch: Code Injection/DDOS Hardening**

    - Implementation of HTTP Request Limit on the web server
    - These limits may include elements such as:

        - Maximum URL Length
        - Maximum length of a query string
        - Maximum size of a request

    - Implementation of input validation on forms

- **Why It Works:**

    - If an HTTP requests URL length, query string and or size limits exceed the set request limits, an error alert will trigger and helps to rejects too large requests.
    - Input validation can help protect against malicious data anyone attempts to send to the server via the website or application in/across a HTTP request.

Vulnerability – 3 CPU Usage Monitor

- **Patch: Virus or Malware Hardening**

    - Add or update to a antivirus software
    - Implement and configure Host Based Intrusion Detection System (HIDS)

- **Why It Works:**
    - Antiviruses specialize in removal, detection and overall prevention of malicious threats against computers.

        - Any modern antivirus usually covers more than viruses and are a robust solution to protecting a computer in general.

    - HIDS monitors and analyses internals of computing systems.

        - They also monitor and analyse network packets.