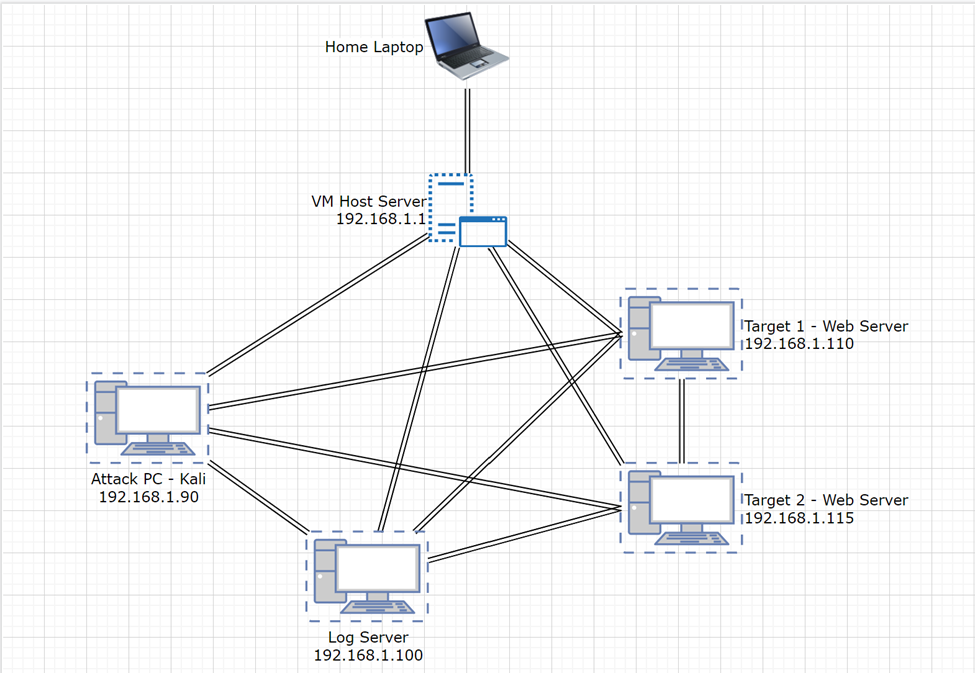
# Blue Team: Summary of Operations

## Network Topology



**VM Host Server**

* Operating System: Windows 10
* Purpose: Host other VM’s
* IP Address: 192.168.1.1

**Kali**

* Operating System: Linux
* Purpose: Attack PC
* IP Address: 192.168.1.90

**Log Server - ELK**

* Operating System: Linux
* Purpose: Log Server
* IP Address: 192.168.1.100

**Target 1**

* Operating System: Linux
* Purpose: Target PC
* IP Address: 192.168.1.110

**Target 2**

* Operating System: Linux
* Purpose: Target PC
* IP Address: 192.168.1.115

## Description of Targets

* Two VMs on the network were vulnerable to attack:
  + Target 1 192.168.1.110
  + Target 2 192.168.1.115
* Each VM functions as an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers.

## Monitoring the Targets

This scan identifies the services below as potential points of entry:

Text

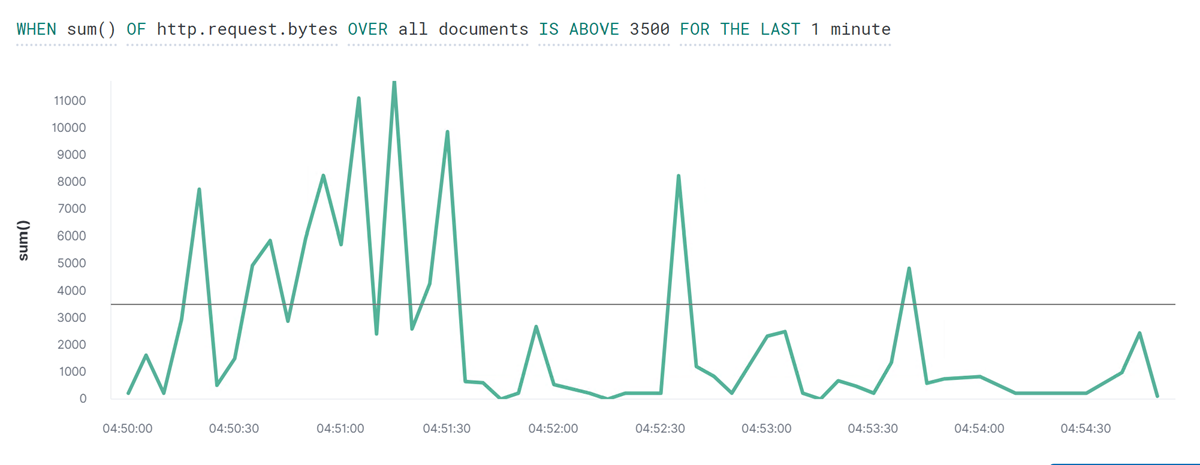
Description automatically generated

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

**Alert 1:**

Sum of HTTP Requests in Bytes is implemented as follows:

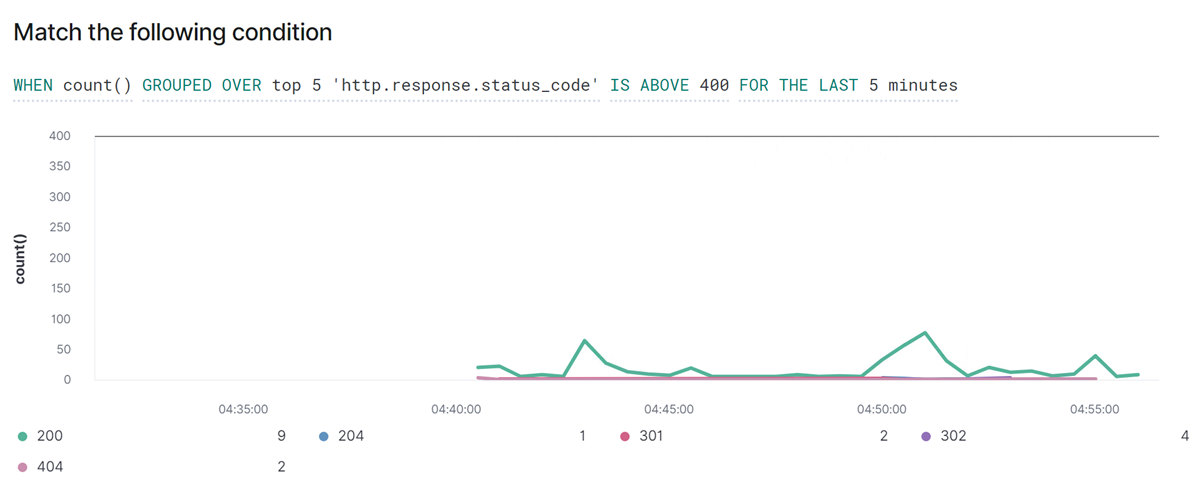
* Metric: Sum of http.request.bytes over all documents
* Threshold: above 3500 for the last minute
* Vulnerability Mitigated: port scans
* Reliability: medium



**Alert 2**

Count of HTTP response codes is implemented as follows:

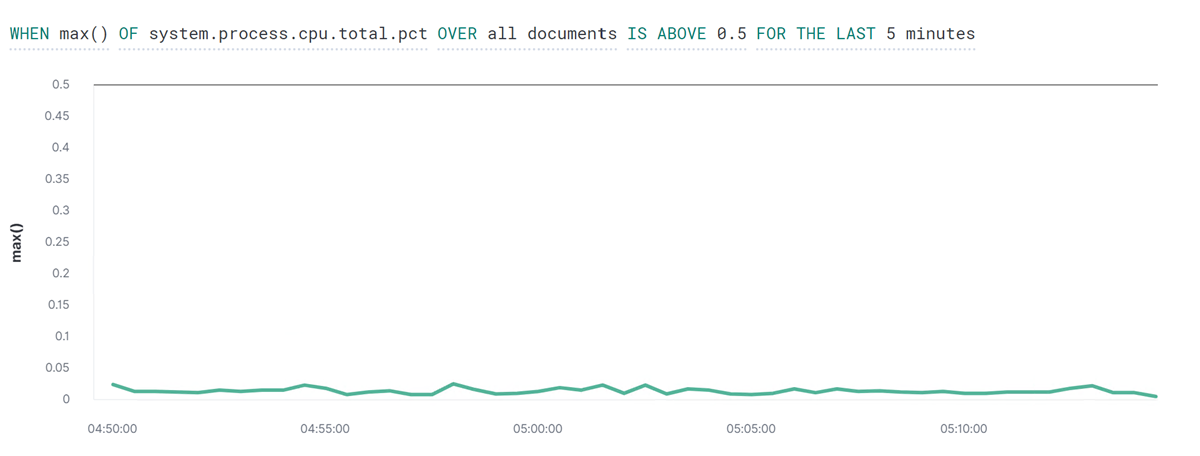
* Metric: When count count grouped over top 5 is http\_response\_status\_code
* Threshold: Above 400 for last 5 mins
* Vulnerability Mitigated: failed attempts to access files/folders
* Reliability: High

[INSERT: An image of the alert being fired.]

**Alert 3**

CPU system process use is implemented as follows:

* Metric: when max of system.process.cpu.total.pct over all documents
* Threshold: Above .5 for last 5 mins
* Vulnerability Mitigated: use of target as a slave or miner
* Reliability: Medium



## Suggestions for Going Further

**Vulnerability 1**

**CVE-2020-4049:** In affected versions of WordPress, when uploading themes, the name of the theme folder can be crafted in a way that could lead to JavaScript execution in /wp-admin on the themes page. This does require an admin to upload the theme, and is low severity self-XSS. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

**Rating: 2.4 Low**

**Mitigation:** Upgrade Wordpress to version 5.4.2. This version has patched the vulnerability

**Vulnerability 2**

**CVE-2016-6210:** sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

**Rating: 5.9 Medium**

**Mitigation:** Upgrade OpenSSH to version 7.3 or later. Patched version.

**CVE-2016-6515:** The auth\_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.

**Rating**: **7.5 High**

**Mitigation:** Upgrade OpenSSH to version 7.3 or later. Patched version.

**CVE-2015-8325:** The do\_setup\_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam\_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD\_PRELOAD environment variable.

**Rating: 7.8 High**

**Mitigation:** Upgrade OpenSSH to version 7.3 or later. Patched version.

**CVE-2015-5600:** The kbdint\_next\_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.

**Rating: N/A**

**Mitigation:** Upgrade OpenSSH to version 7.3 or later. Patched version.

**Vulnerability 3**

**CVE-2017-7679:** In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod\_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

**Rating: 9.8 CRITICAL**

**Mitigation:** Upgrade Apache to version 2.4.26 or later

**CVE-2017-7668:** The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap\_find\_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap\_find\_token() to return an incorrect value.

**Rating: 9.8 CRITICAL**

**Mitigation:** Upgrade Apache to version 2.4.26 or later

**CVE-2017-3169:** In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod\_ssl may dereference a NULL pointer when third-party modules call ap\_hook\_process\_connection() during an HTTP request to an HTTPS port.

**Rating: 9.8 CRITICAL**

**Mitigation:** Upgrade Apache to version 2.4.26 or later

**CVE-2017-3167:** In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap\_get\_basic\_auth\_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

**Rating: 9.8 CRITICAL**

**Mitigation:** Upgrade Apache to version 2.4.26 or later