# 

# 

# 

# **Blue Team:**

# **Summary of Operations**

## 

## By Dean Baberowski

## 

## 

## 

## 

## 

## 

## Table of Contents

[Network Topology](#_zbg9g1fdodti) 3

[Description of Targets](#_pkqjm54q3b9u) 3

[Monitoring the Targets](#_nzifd14pmrv9) 4

[Suggestions for Going Further](#_9ah1al4q58uf) 7

## 

## 

## 

## 

## 

## 

## **Network Topology**

The following machines were identified on the network:

**Kali Linux**

Operating system: Kali Linux

Purpose: attacking machine

IP Address: 192.168.1.90

**Target 1**

* Operating System: Linux
* Purpose: Web server running Wordpress
* IP Address: 192.168.1.110

**Target 2**

* Operating System: Linux
* Purpose: Web server running Wordpress
* IP Address: 192.168.1.115

Including a Gliffy or draw.io diagram is optional but highly encouraged.

## Description of Targets

* Two VMs on the network were vulnerable to attack: Target 1 192.168.1.110 and 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:

* **Target 1**

1. SSH Vulnerability CVE-1999-0398 - high severity
2. RPC bind #10000 CVE 2017-8779 Medium
3. SQL Injection - CWE 422 - Medium Allows attackers to inject an SQL database.
4. Wordpress Vulnerability CVE-2009-3891 Low

* **Target 2**

1. SSH Vulnerability CVE-1999-0398 - high severity
2. SQL Injection - CWE 422 -Medium Allows attackers to inject an SQL database.
3. RPC bind #10000 CVE 2017-8779 Medium

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

**HTTP Request size Monitor**

HTTP Request size monitor is implemented as follows:

* Metric: HTTP.request
* Threshold: IS Above 400
* Vulnerability Mitigated: To monitor excessive HTTP requests
* Reliability: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability

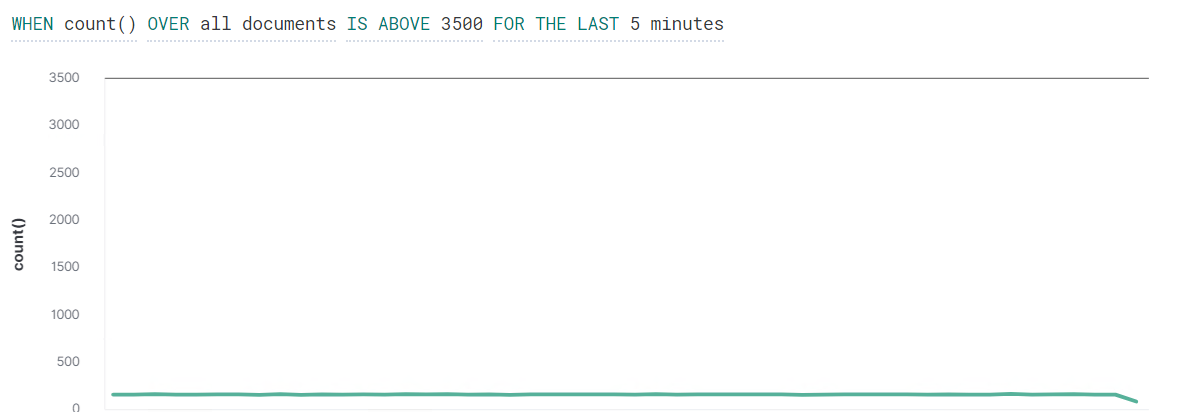
This alert creates a lot of false positives as the data is generated as the machine is attacked. It has medium reliability.



**Excessive HTTP Errors**

Excessive HTTP Errors is implemented as follows:

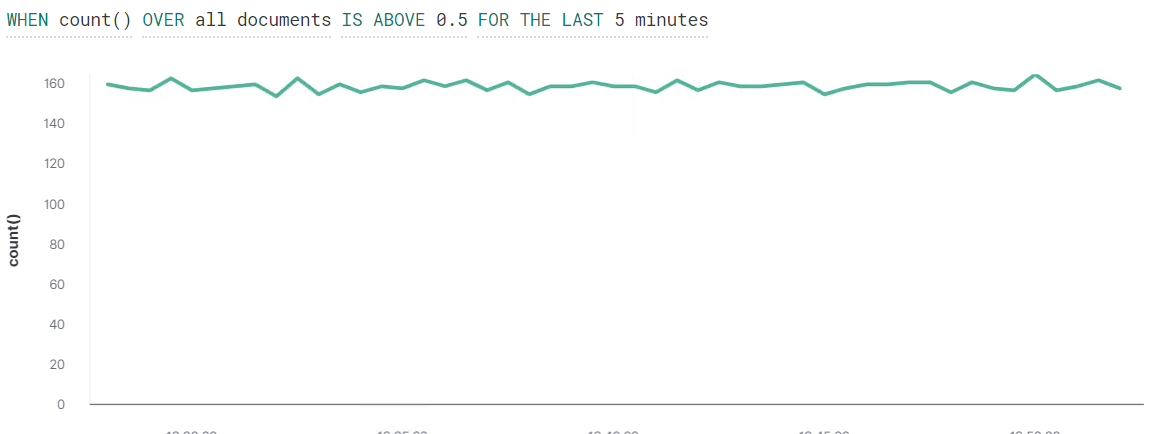
* Metric: HTTP.errors
* Threshold: 3500
* Vulnerability Mitigated: To stop excessive errors from being generated
* Reliability: The alert generates a high reliability as it depends on how many HTTP errors are being generated on the system.



**CPU Usage monitor**

CPU Usage monitor is implemented as follows:

* Metric: cpu.usage
* Threshold: Above 0.5
* Vulnerability Mitigated: To monitor high activity on the network
* Reliability: Medium reliability



## 

## 

## 

## 

## **Suggestions for Going Further**

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats. 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:

**Wordpress Vulnerability**

* Patch: use wget <http://wordpress.org/latest.zip> to get the latest wordpress update
* Why It Works: Wordpress releases updates and the third parties release updates weekly.

**SSH Vulnerability**

* Patch: use install apt-get install fail-to-ban
* Why It Works: use fail-2-ban to block access to SSH port

**High CPU usage**

* Patch: Update the drivers using apt-get <name of driver>
* Why It Works: Drivers get updated monthly or weekly depending on the manufacturer.