BLUE TEAM SUMMARY OF OPERATIONS

MONITORING, ANALYSIS AND MITIGATION OF A VULNERABLE NETWORK

TABLE OF CONTENTS

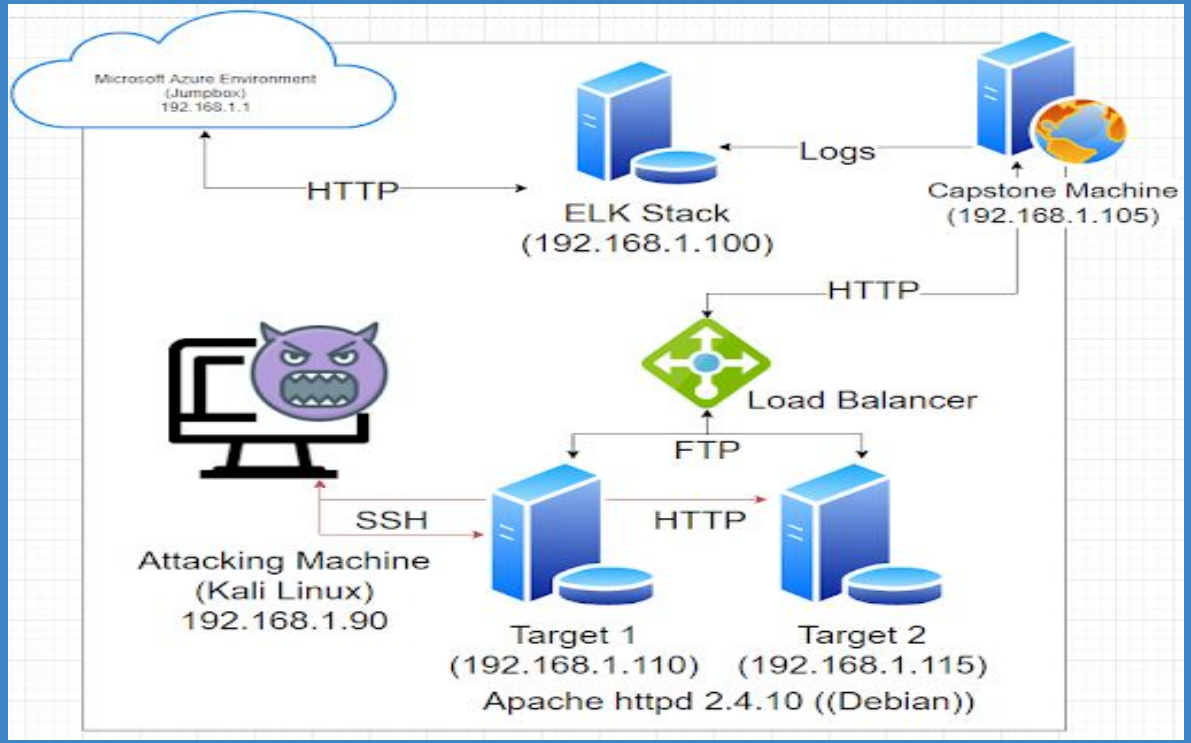
This document contains the following resources:

Blue Team Operations

Defenders of the System

- Analysis of Information Systems to ensure security
- Identify security flaws
- Implement and Verify effective security measures
- Continue monitoring of the system to ensure system security

NETWORK TOPOLOGY



Network
Address Range: 192.168.1.1/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Linux Kali 5.4.0-kali3
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu 18.04.4 LTS
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.04.4 LTS
Hostname: ELK

IPv4: 192.168.1.110
OS: debian 3.16.0-6-amd64
Hostname: Target 1

IPv4: 192.168.1.115
OS: debian 3.16.0-6-amd64
Hostname: Target 2

DESCRIPTION OF TARGETS:

[TARGET1]

- Operating System: Linux (Apache httpd 2.4.10 (Debian))
- Purpose: Apache Web Server/Wordpress Redundancy
- IP Address: 192.168.1.110

[TARGET2]

- Operating System: Linux (Apache httpd 2.4.10 (Debian))
- Purpose: Apache Web Server/Wordpress Redundancy
- IP Address: 192.168.1.115

- 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.

OTHER MACHINES:

[ATTACKING MACHINE]

- Operating System: Kali Linux
- Purpose: Threat Actor
- IP Address: 192.168.1.90

[ELK Stack]

- Operating System: Ubuntu Linux
- Purpose: Data Ingestion, Logging, Systems Analysis Intrusion Detection System
- IP Address: 192.168.1.100

[Capstone]

- Operating System: Ubuntu Linux
- Purpose: Sending logs to ELK Stack/Apache Web Server
- IP Address: 192.168.1.105

[Azure Machine]

- Operating System: Microsoft Windows RPC
- Purpose: Jump Box/Azure Cloud Environment
- IP Address: 192.168.1.1

Monitoring the Targets:

Identified ports and associated services as potential points of entry:

- **Target 1**
  - Port 22/tcp - ssh
  - Port 80/tcp - http
  - Port 111/tcp - rpcbind
  - Port 139/tcp - netbios-ssn Samba
  - Port 445/tcp - netbios-ssn Samba

- **Target 2**
  - Port 22/tcp - ssh
  - Port 80/tcp - http
  - Port 111/tcp - rpcbind
  - Port 139/tcp - netbios-ssn Samba
  - Port 445/tcp - netbios-ssn Samba

Monitoring the Targets:

ELK Stack Server/ Apache Server

ELK STACK SERVER: OPEN SOURCE DATA MANAGEMENT TOOL

Elasticsearch, **L**ogstash, and **K**ibana. **Elasticsearch** is a search and analytics engine. **Logstash** is a server-side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch. **Kibana** lets users visualize data with charts and graphs in Elasticsearch.

- DATA STORAGE
- SEARCH and ANALYTICS ENGINE
- DATA ANALYSIS
- VISUALIZATION OF DATA ANALYSIS
- REAL TIME SYSTEMS MONITORING DASHBOARD
- **I**ntrusion **D**etection **S**ystem (**IDS)** capable

ELK MONITORING TOOLS

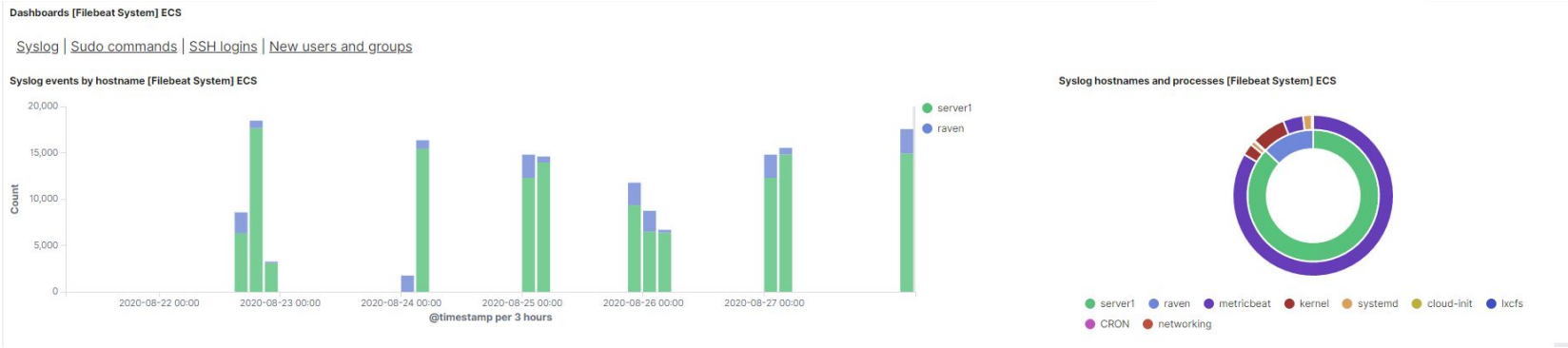
Primary Monitoring Tools Utilized in Kibana

FILEBEAT - Monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

PACKETBEAT - A real-time network packet analyzer that you can use with Elasticsearch to provide an application monitoring and performance analytics system.

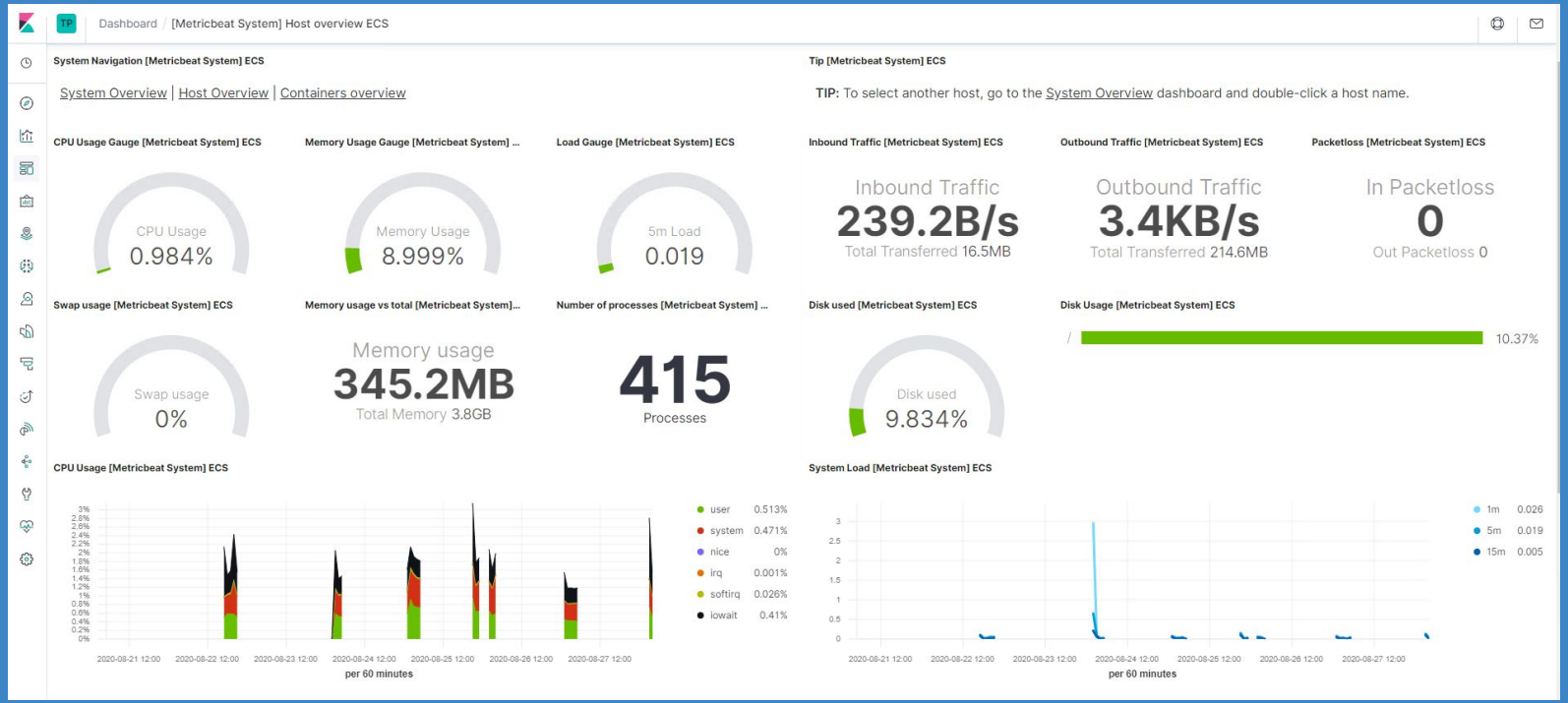
METRICBEAT - Collect metrics from the operating system and from services running on the server.

Filebeat Dashboard



KIBANA DASHBOARD

Visualize Your monitoring systems



Packetbeat Dashboard

Visualization of HTTP Traffic

MONITORING THE TARGETS:

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

Name of Alert 1

Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

- Metric: Excessive HTTP Errors WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- Threshold: exceeds 400/ 5minutes
- Vulnerability Mitigated:
- Reliability: high reliability.

ID	Name	State	Last fired	Last triggered
cd6b411f-14f0-4438-be6b-68fb0825b229	Excessive HTTP Errors	✓ OK	2 days ago	a few seconds ago

Name of Alert 2

HTTP Request Size

Request Size Monitor is implemented as follows:

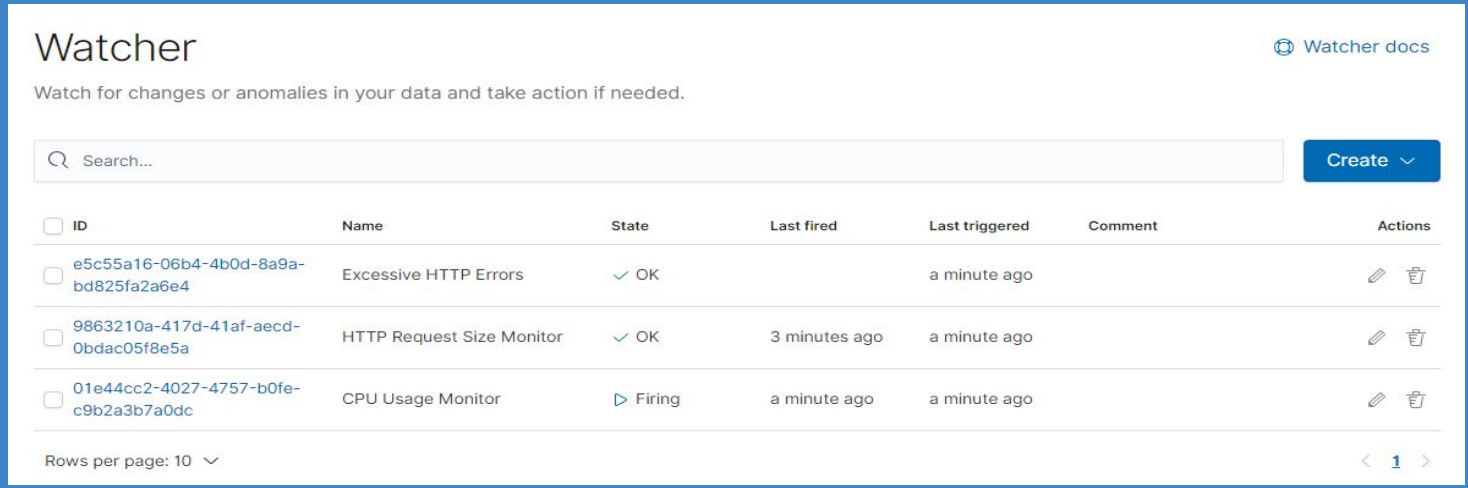
- Metric: HTTP Request Size Monitor WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- Threshold: Sum Exceeds 3500 bytes in the last 1minute
- Vulnerability Mitigated:
- Reliability: high reliability, if baseline and thresholds are set correctly

Name of Alert 3

CPU Usage Monitor

CPU usage is implemented as follows:

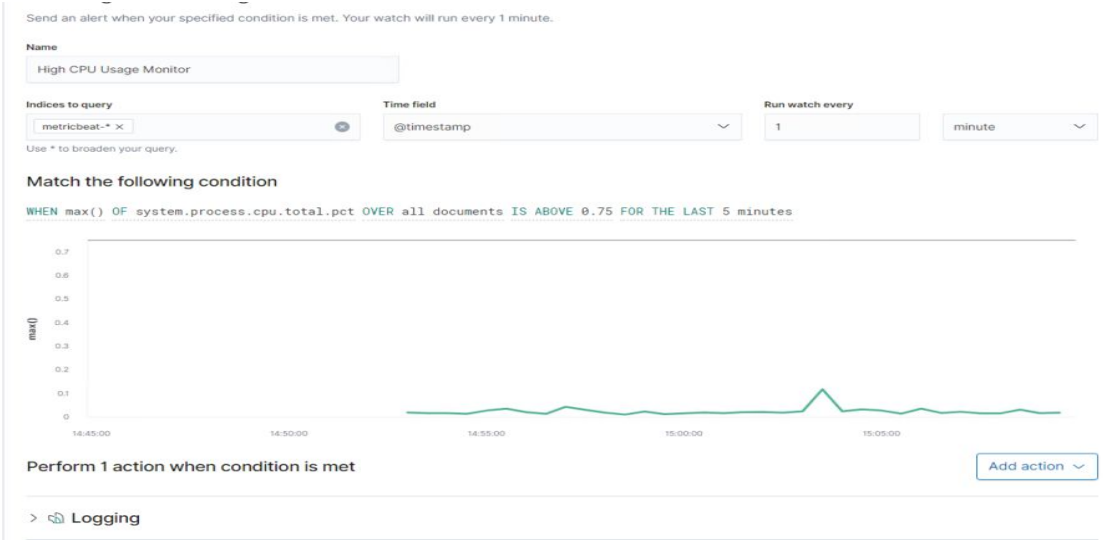
- Metric: CPU Usage WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- Threshold: Exceeds 0.5 % of total system processes for the last 5 minutes
- Vulnerability Mitigated:
- Reliability: TODO: high reliability.



Name of Alert 4
High CPU Usage Monitor

CPU usage is implemented as follows:

- Metric: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.75 FOR THE LAST 5 minutes
- Threshold: Exceeds 75% of total system processes for the last 5 minutes
- Vulnerability Mitigated: added alert to show higher usage
- Reliability: high reliability.

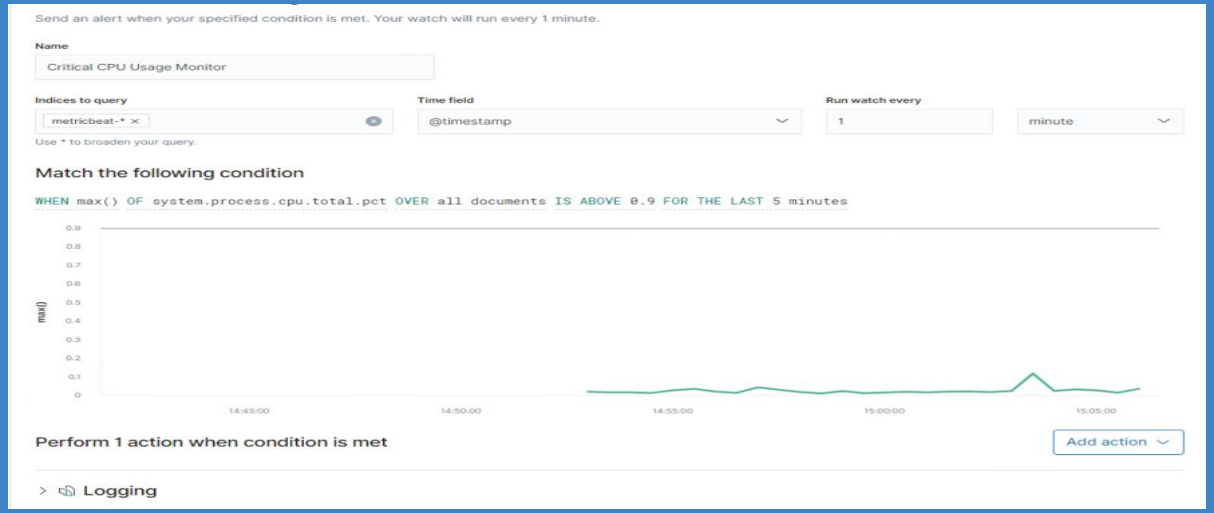


Name of Alert 5

Critical CPU Usage Monitor

CPU usage is implemented as follows:

- Metric: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.9 FOR THE LAST 5 minutes
- Threshold: Exceeds 90% of total system processes for the last 5 minutes
- Vulnerability Mitigated: added alert to show critical usage
- Reliability: high 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:

Vulnerability 1: Port 111 (Portmapper) rpcbind

- Patch: install `special-security-package` with `apt-get`
- Why It Works: `special-security-package` scans the system for viruses every day
- Other suggestions: add IPTables to deny TCP connection of unwanted IP ranges

Vulnerability 2: Port 139 (NetBIOS) NBSTAT

- Patch: chmod 600 /var/www/html/wordpress/wp-config.php
- Why It Works: By changing the permissions on the config file, only the owner would have full access while all other privileges would be denied to all outside users.
- Other suggestions: turn off File and Print Sharing, block ports 137-139 completely or use strong passwords

Vulnerability 3: Port 445 (SMB)

- Patch: restrict access to TCP port 445 (SMB)
- Why it Works: Prevents file and printer sharing from unauthorized users
- Other suggestions: delete HKLM\System\CurrentControlSet\Services\NetBT\Parameters\TransportBindName (value only) in the Windows Registry