Final Engagement

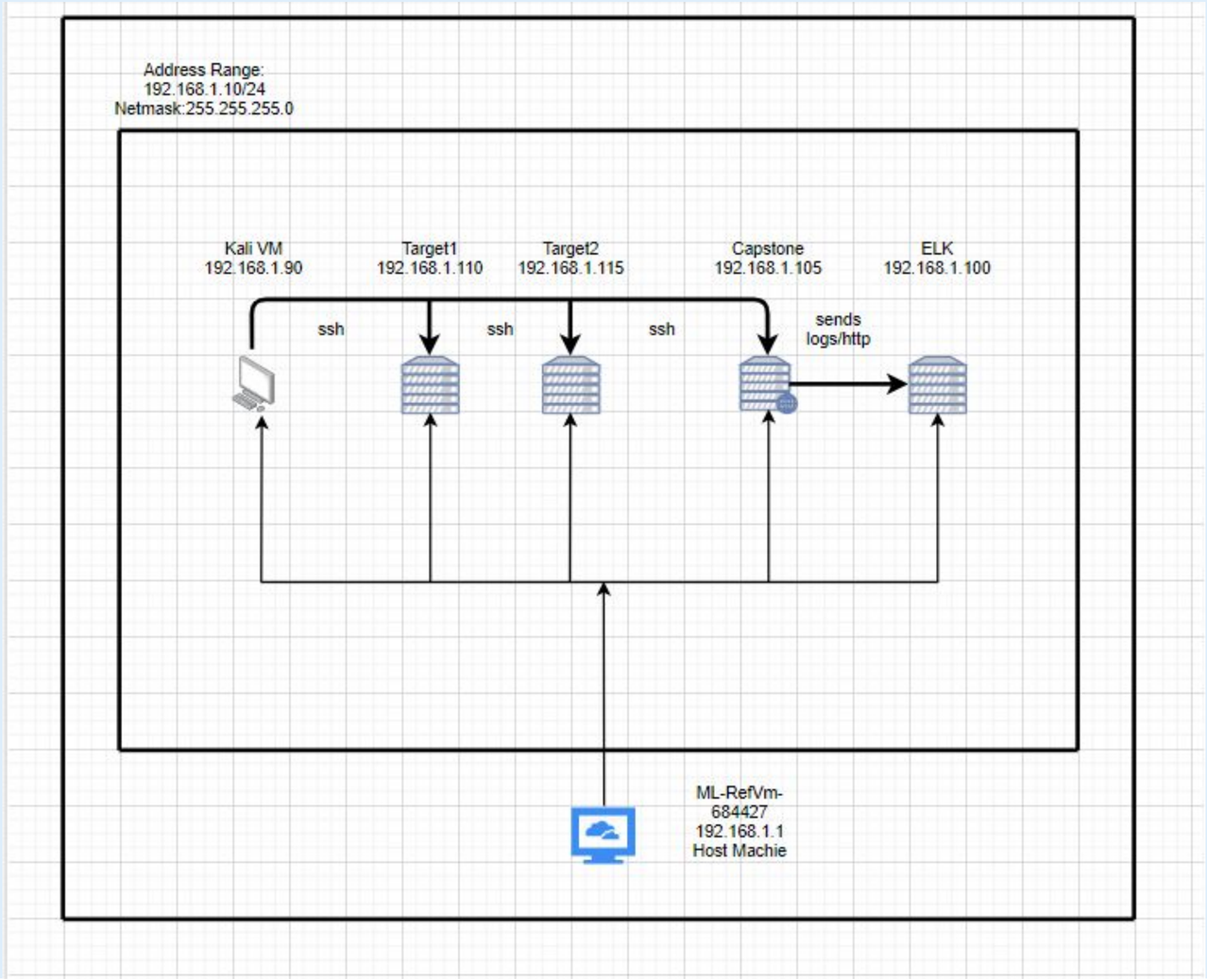
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask:
Gateway:255.255.255.0

Machines
IPv4: 192.168.1.90
OS: Kali/Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Debian/Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04 1 LTS
Hostnamne:
Capstone/server1

IPv4: 192.168.1.110
OS: Debian/Linux 8 (jessie)
Hostname: taget1

IPv4: 192.168.1.115
OS: Debian/Linux 8 (jessie)
Hostname: target 2

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Password Vulnerability	Michael used simple password	The simple password enabled access to other sensitive data
CVE-2015-5600	Remote attackers to conduct brute-force attacks	Attacker is able to request as many password prompts limited by the "login graced time" setting that is set to two minutes by default."
Sensitive Data Mismanagement	Sensitive data was being stored on public facing website	Flag3 was located on public blog post

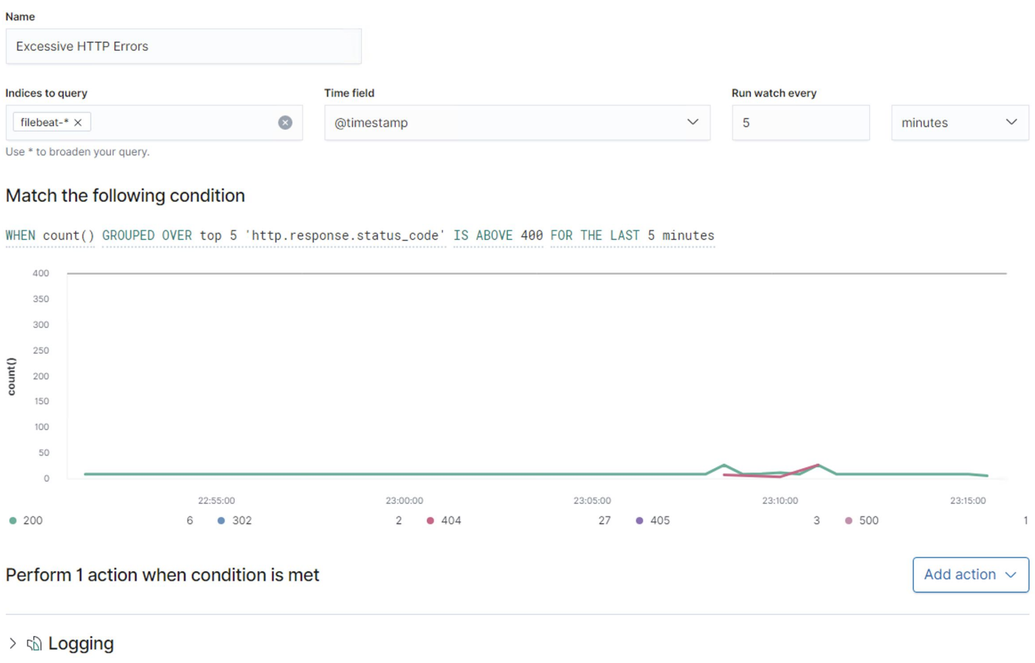
Alerts Implemented

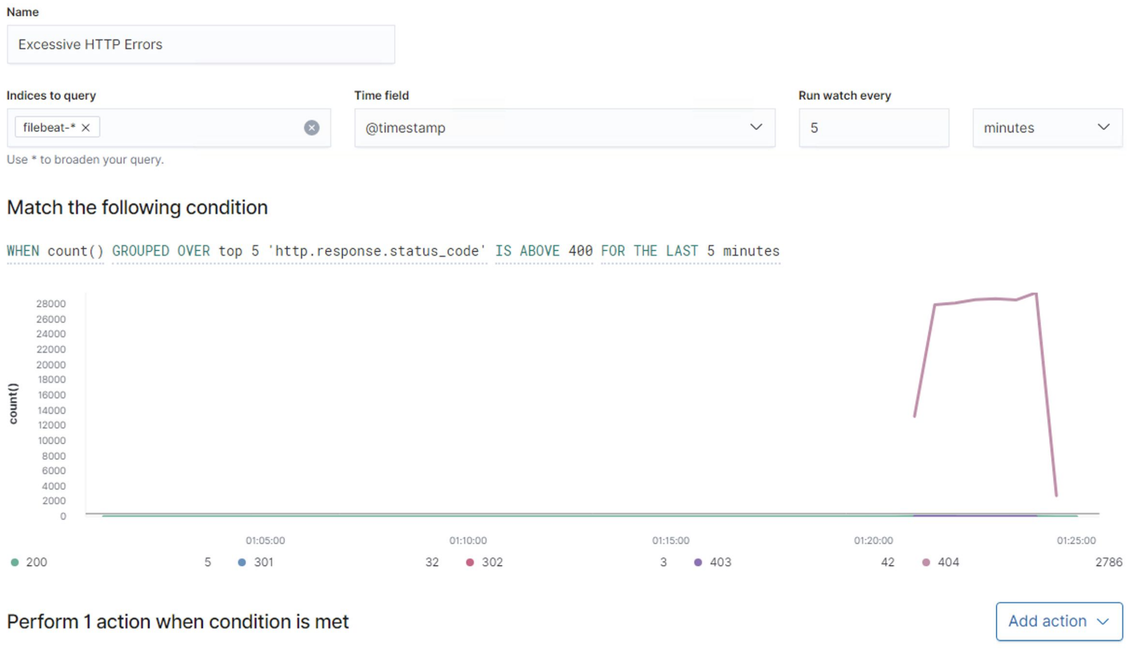
Excessive HTTP Errors

- Which **metric** does this alert monitor?

  Top 5 HTTP Error response codes grouped together
- What is the **threshold** it fires at?

  400 for the last 5 minutes
- Provide a screenshot of the alert in action.



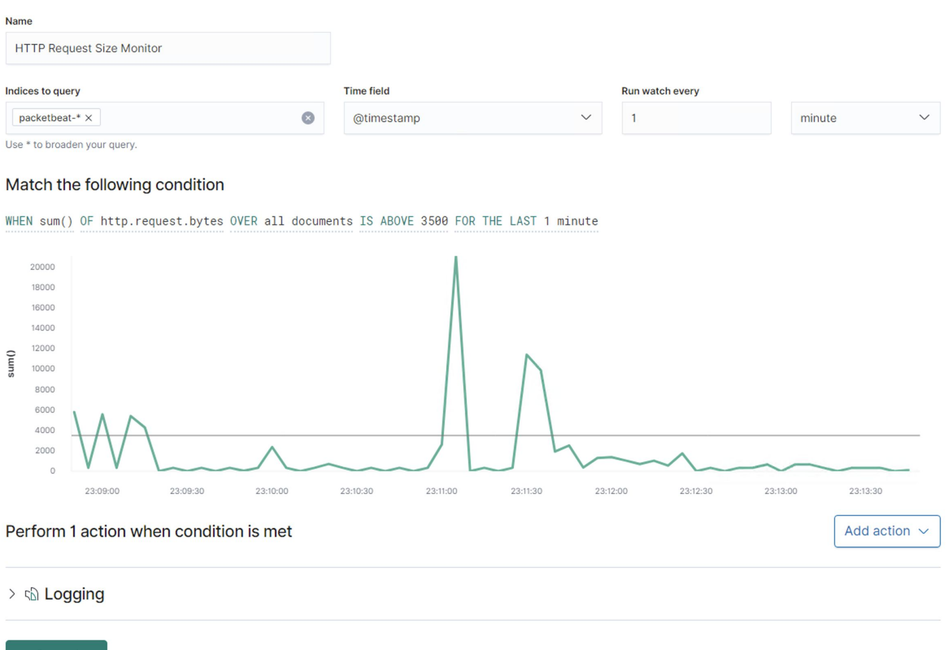


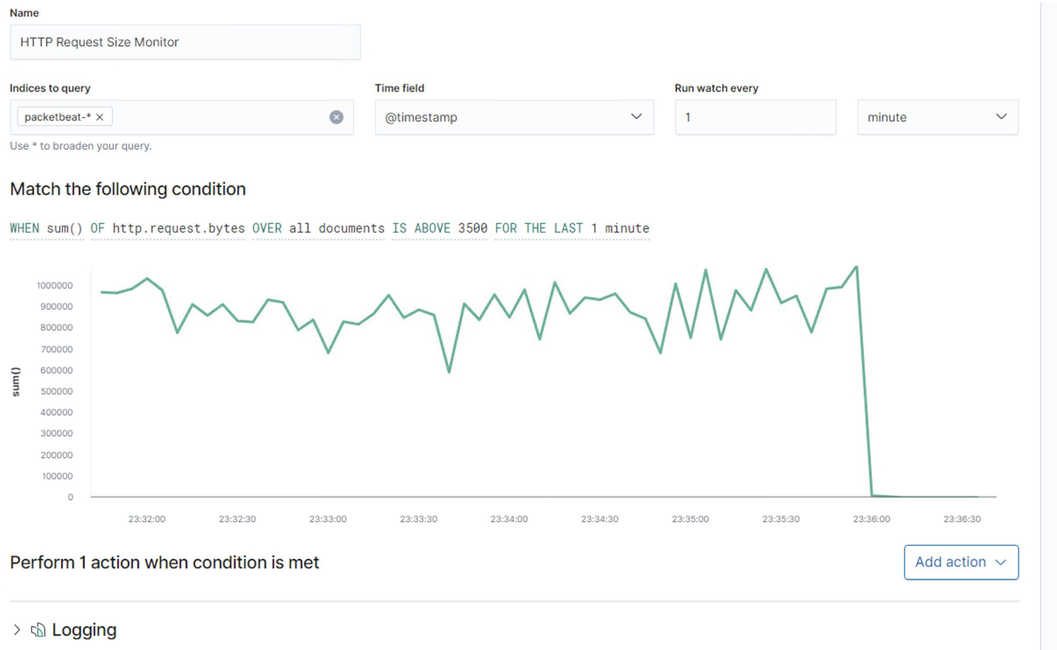
HTTP Request Size Monitor

- Which **metric** does this alert monitor?

  The sum of HTTP requests over all documents
- What is the **threshold** it fires at?

  Above 3500 for the last 1 minute
- Provide a screenshot of the alert in action.



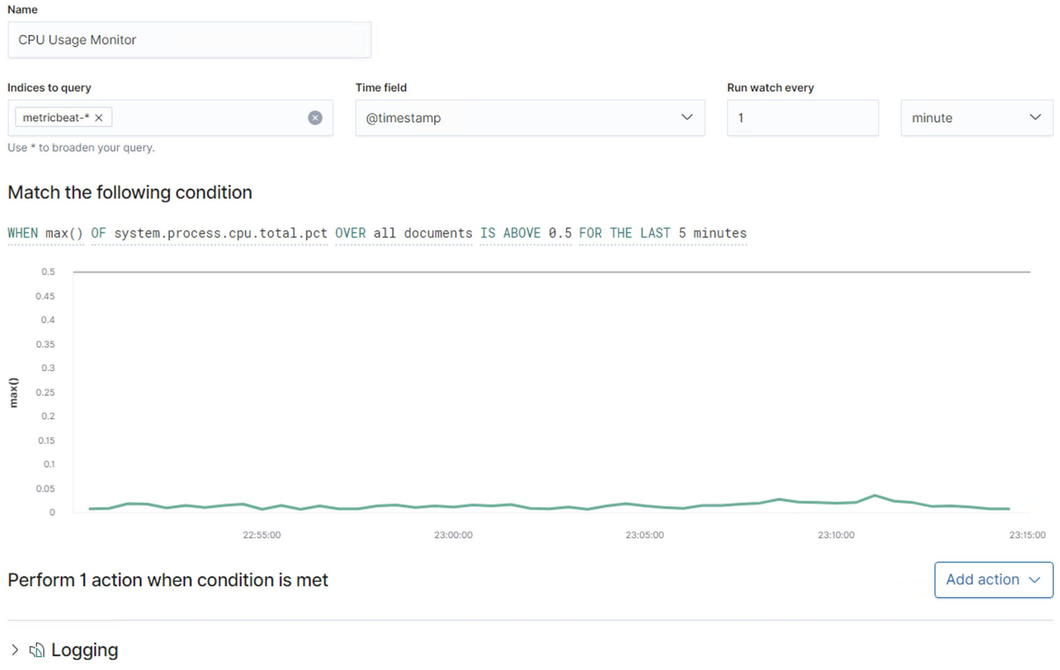


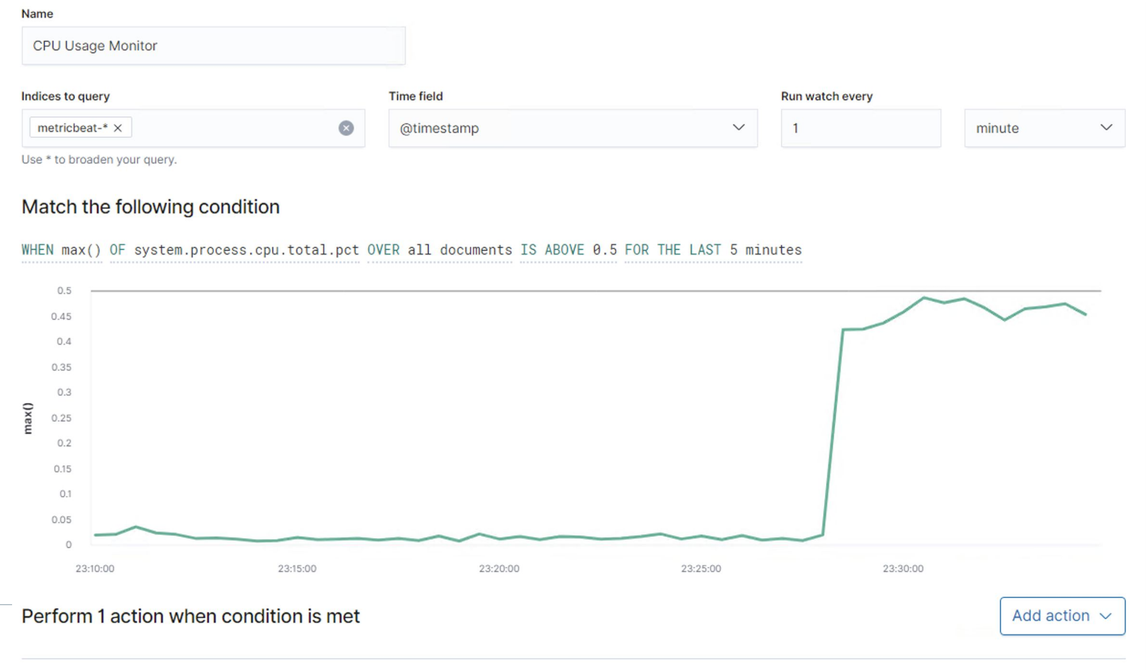
CPU Usage Monitor

- Which **metric** does this alert monitor?

  The system process cpu total level over all documents
- What is the **threshold** it fires at?

  0.5 over the last 5 minutes
- Provide a screenshot of the alert in action.





Hardening

Hardening: Simple password vulnerability on Target 1

Administrative controls:

- OWASP Top 10 #2 || Critical
- Unique password requirements:
  - 12 character length, 3 different type of characters, etc
- Password reset requirement:
  - Every 60 days

Hardening Against CVE-2015-5600 on Target 1

- Vendor: OpenBSD, Product: OpenSSH (OpenBSD Secure Shell), Version: 6.9
- Install recent security update or OS for systems such as:
  - Apple Mac OSX 10.10.0-4
  - CentOS 6,7
  - IBM Security Network Protection 5.2.0, 5.3.1, 5.2.0
  - OpenSSH openSSH 6.9p1
  - MacAfee Web Gateway 7.x.x.x
  - Ubuntu Linux 12.04 LTS amd64, LTS i386, 14.04 LTS, 15.04

- How to install it examples:

Install Mac OSX update 10.10.5

Linux Ubunu: `sudo apt update && sudo apt upgrade -y`

Hardening Against Sensitive Data Management on Target 1

Employee Training

- OWASP Top 10 #3 || Critical
- Sensitive data needs to be stored in well secured password protected directories on the server.
- Places such as blog posts on a WordPress site are not safe areas for sensitive data
- As we have seen, there are many HTTP port 80 vulnerabilities using open source software to design web sites and they need to be mitigated actively.

Implementing Patches

Implementing Patches with Ansible

Example

Playbook Overview

CVE-2015-5600

```yaml
---
- hosts: servers
  become: true
  become_user: root
  tasks:
    - name: Update apt repo and cache on all Debian/Ubuntu boxes
      apt: update_cache=yes force_apt_get=yes cache_valid_time=3600

    - name: Upgrade all packages on servers
      apt: upgrade=dist force_apt_get=yes

    - name: Check if a reboot is needed on all servers
      register: reboot_required_file
      stat: path=/var/run/reboot-required get_md5=no

    - name: Reboot the box if kernel updated
      reboot:
        msg: "Reboot initiated by Ansible for kernel updates"
        connect_timeout: 5
        reboot_timeout: 300
        pre_reboot_delay: 0
        post_reboot_delay: 30
        test_command: uptime
      when: reboot_required_file.stat.exists
```

[Start of Network Analysis]