Final Engagement

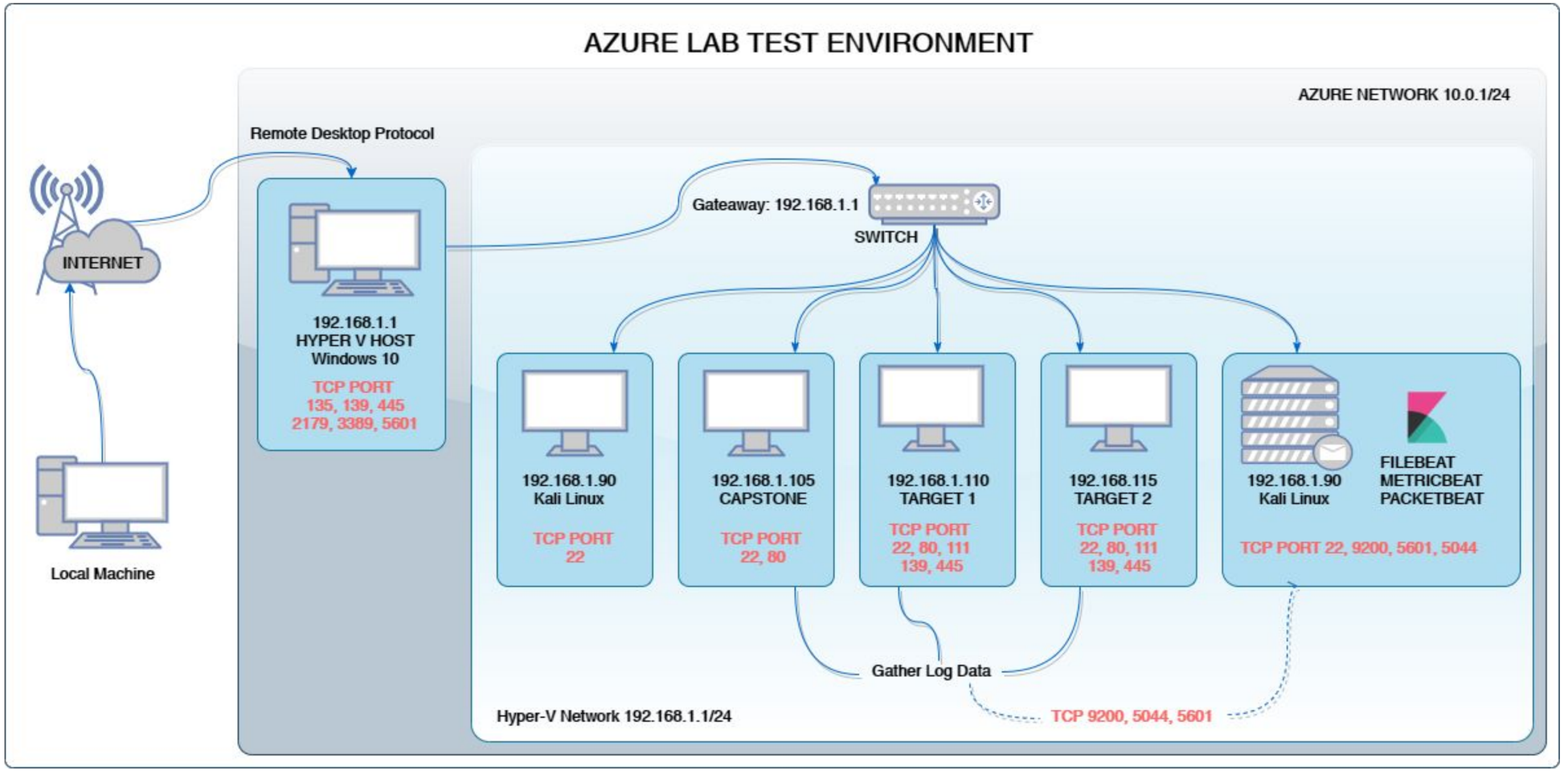
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address
Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.100
OS: Ubuntu 18.04.1 LTS
Hostname: ELK

IPv4: 192.168.1.100
OS: Ubuntu 18.04.1 LTS
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux 3.2-4.9
Hostname: Target 1

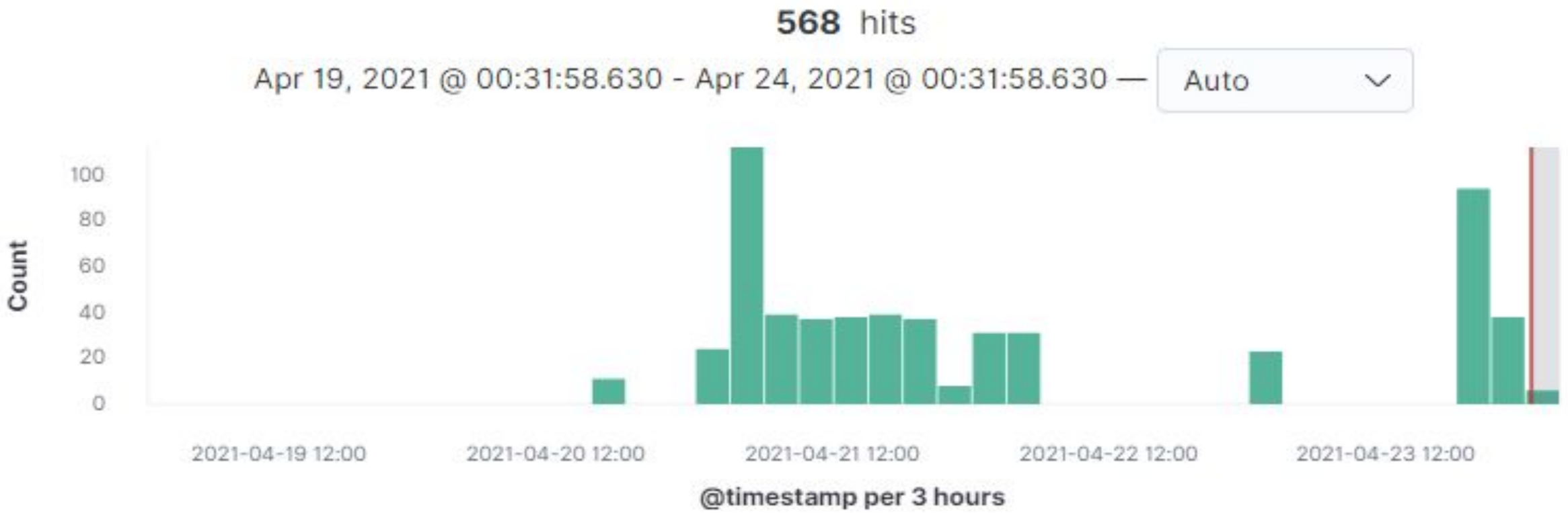
IPv4: 192.168.1.115
OS: Linux 3.2-4.9
Hostname: Target 2

Alerts Implemented

Excessive HTTP Errors

Summarize the following:

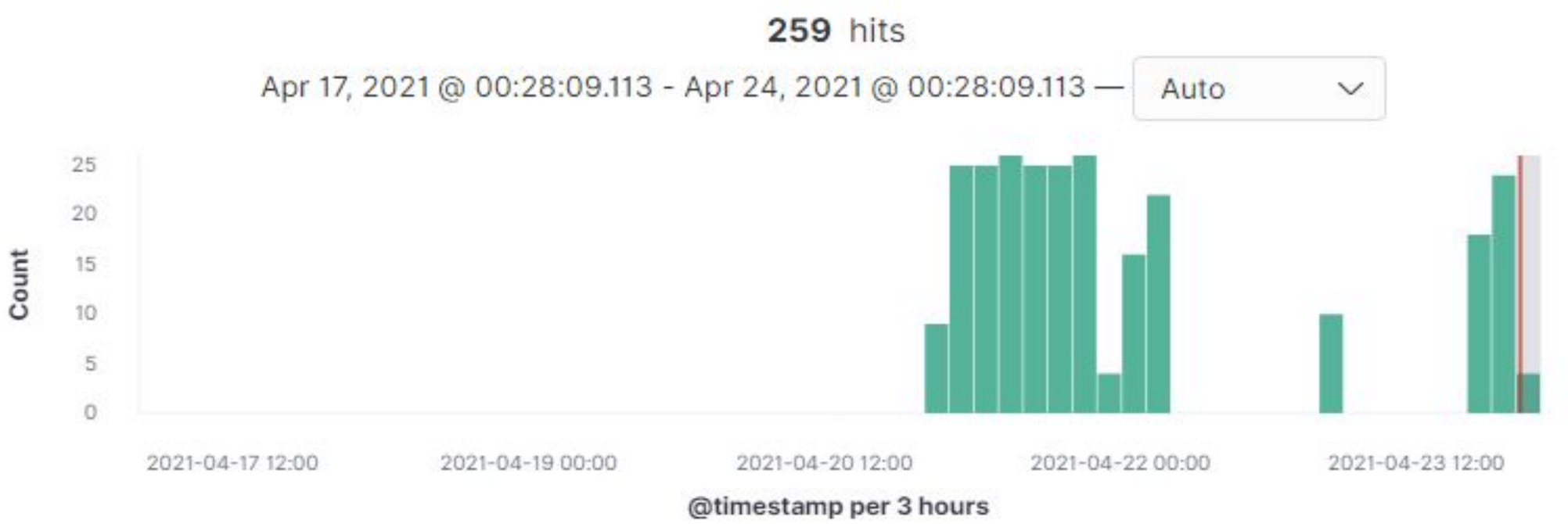
- Packetbeat
- When count() GROUPED OVER top5 ‘http.response.status_code’ is above 400 for the last 5 minutes



HTTP Request Size Monitor

Summarize the following:

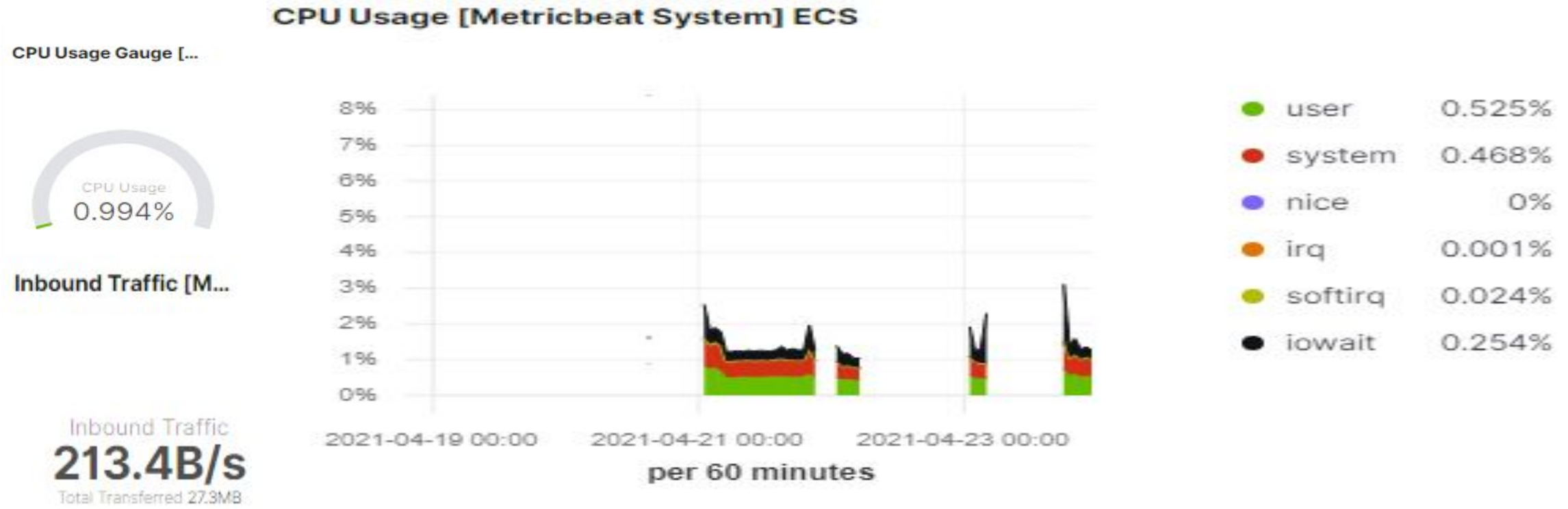
- Packetbeat
- When sum() of http.request.bytes OVER all documents is ABOVE 3500 for the LAST 1 minute



CPU Usage Monitor

Summarize the following:

- Metricbeat
- WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes



Hardening

Hardening Against Open Ports and Weak Passwords on Target 1

- Disable access to Port 22
  - This will block anyone trying to gain access via SSH
- Enable a stronger password policy
  - A stronger password policy would make it harder for attackers to easily guess a user's password. Some restrictions to include can be:

    - Requiring a longer character count e.g. 12 characters

    - Requiring the use of different character types e.g. number, symbol, special character

    - Prohibiting the user's name in the password e.g. user's name is Michael, therefore Michael is not allowed as password

Hardening Against MYSQL access on Target 1

- To guard against access to the MySQL database one of the options is to disable account management statements such as create user, grant, revoke, and set password.To prevent remote clients from connecting over TCP/IP, use the –skip- networking option. Clients then can connect only from the localhost using a socket file on UNIX, or a named pipe or shared memory on Windows. To avoid casual connections from the localhost, use a non-standard socket name at the command prompt.

Hardening Against Escalation to Root on Target 1

To prevent unauthorized users to escalate to root, the sudo privileges need to be more strict. Additionally, users should not have the ability to execute python commands also, due to the spawn command. sudo `python -c 'import pty;pty.spawn("/bin/bash")'` Passwords also need to be hashed and not left in plaintext on files that can be access by other users that don't have sudo privileges.

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

- One could utilize ansible and a cron job to automate system wide updates as well as keep necessary tools up to date. Ansible can also be used to verify system health (ie. ensuring web servers are up and running)

```
---
- name: Update apt-get repo and cache
  hosts: webservers
  apt: update_cache=yes force_apt_get=yes cache_valid_time=3600
  - name: Check if reboot is required
  - register: reboot_required_file
  - stat: path=/var/run/reboot-required get_md5=no
```