Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Presented by

TEAM FATALITY

Aliyiah Brown

Alex Ivezaj

Edgar Argueta

Kris Ellis

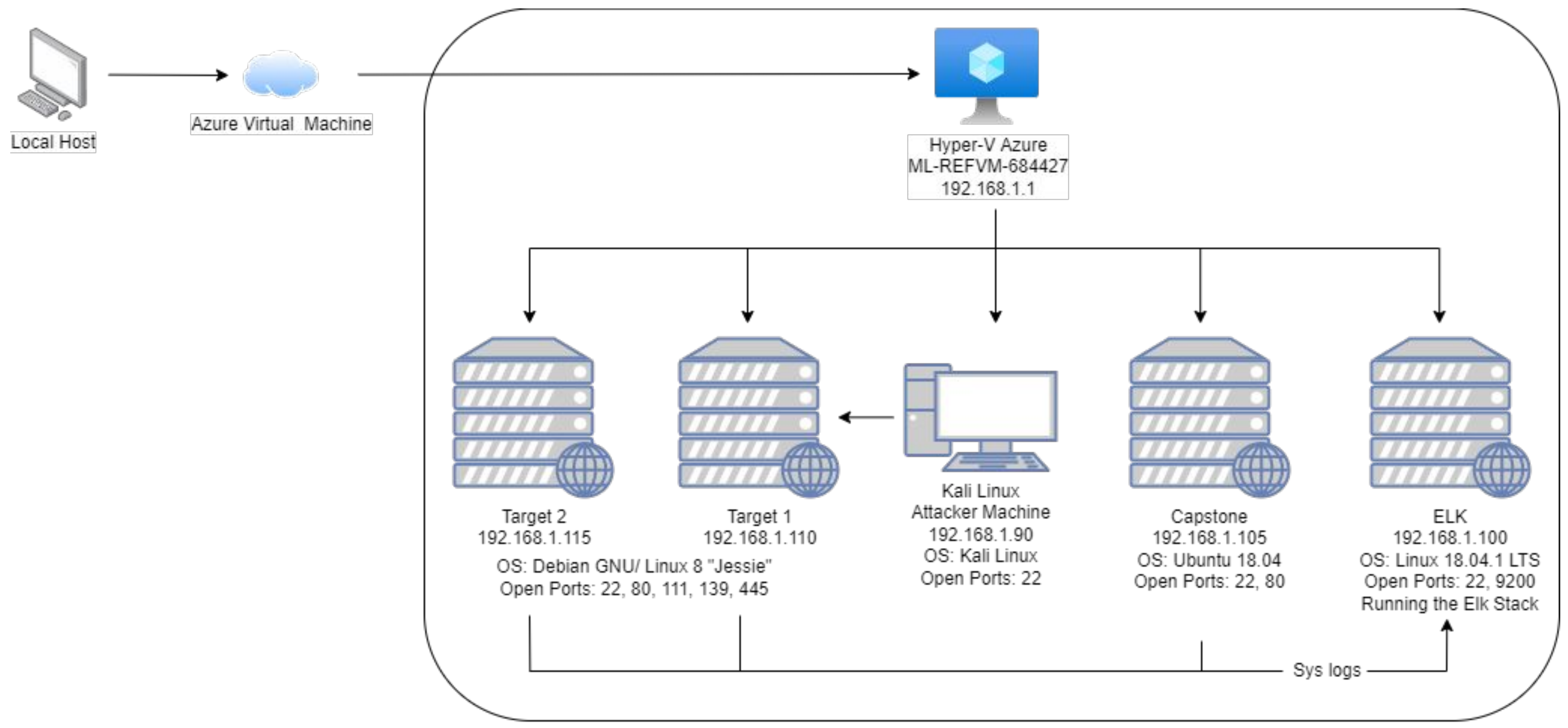
Wade Williams

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
IPv4:192.168.1.105
OS: Ubuntu 18.04
Hostname: Capstone

IPv4: 192.168.1.90
OS: Debian Kali 5.4.0
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: Elk Stack

IPv4: 192.168.1.110
OS: Debian GNU/Linux 8
Hostname: Target 1

Critical Vulnerabilities: Target 1

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

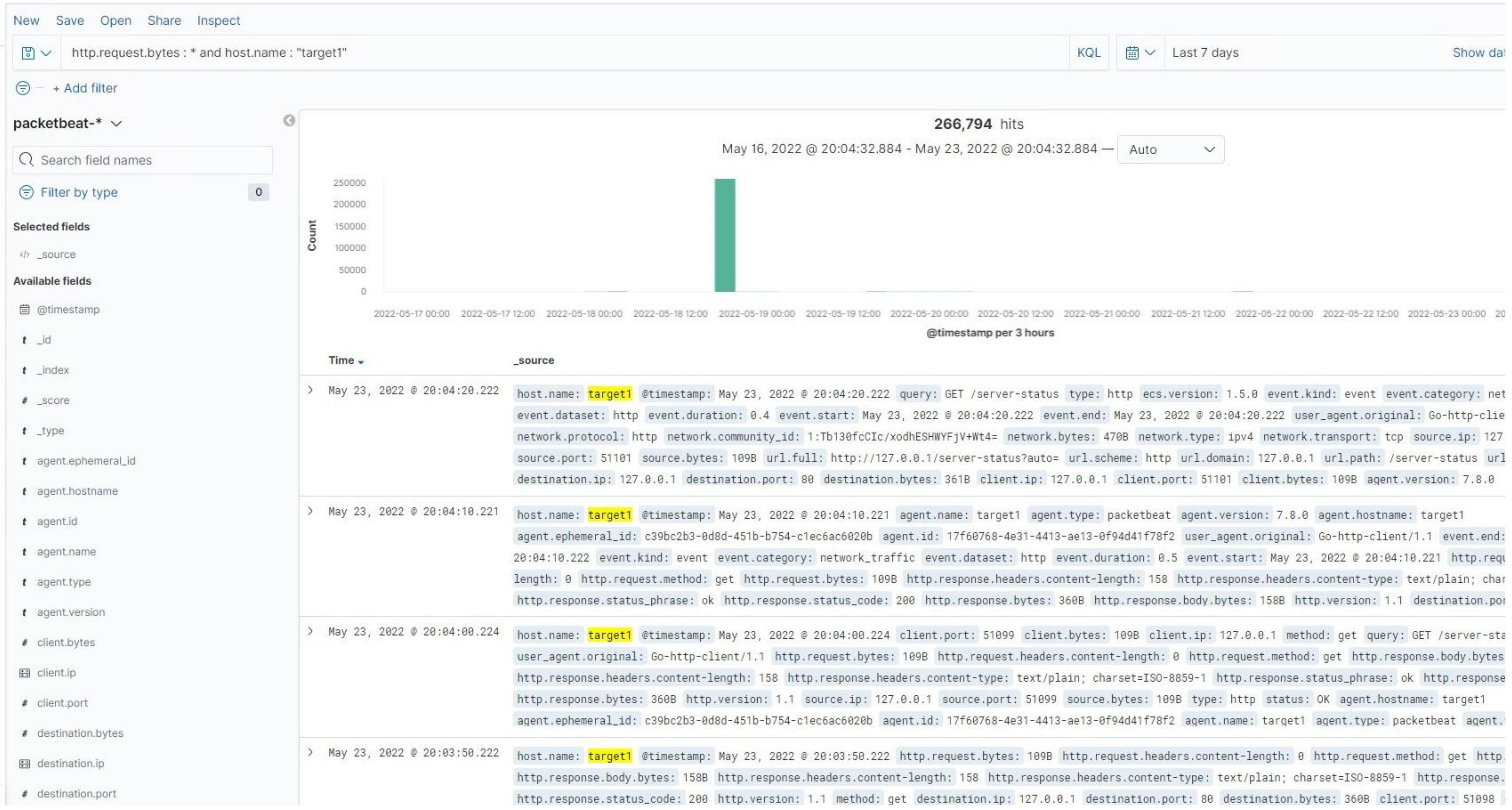
Vulnerability	**Description**	**Impact**
Weak Password	A weak password can have an attacker conduct a simple brute force attack and guess the password.	The attacker can exploit and steal all types of data, spread malware, and ruin the company's reputation.
Mismanaged User Privileges	A user account is given privileges that are not necessary.	The user can perform unauthorized tasks, can gain access to restricted data, or an attacker can have full access to the systems and data.
Unsalted Hash password	A hash password that does not have a unique, random string of characters.	An attacker can easily crack a password through "john" and have unfiltered access to the account.

ALERTS IMPLEMENTED

EXCESSIVE HTTP ERRORS

- WHEN count() GROUPED OVER top 5 'http.response.status_code'
- Threshold: IS ABOVE 400 FOR THE LAST 5 minute

- Response codes 400+ and 500+ are Error codes that warrant attention as they could signal an attack.
- This monitors for enumeration and brute force attacks.



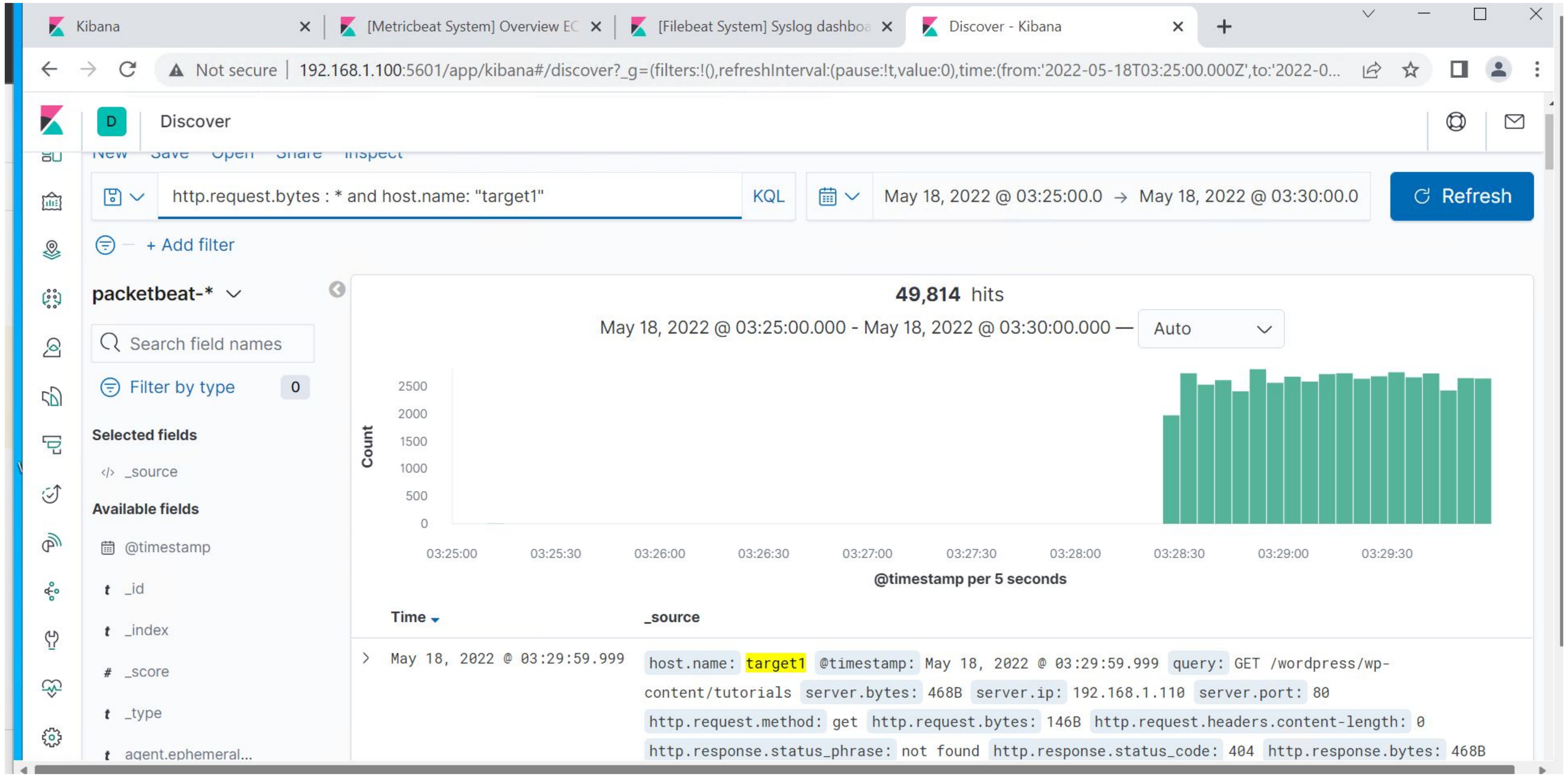
```
http.request.bytes : * and host.name : "target1"

266,794 hits
May 16, 2022 @ 20:04:32.884 - May 23, 2022 @ 20:04:32.884 — Auto
```

```
May 23, 2022 @ 20:04:20.222   host.name: target1 @timestamp: May 23, 2022 @ 20:04:20.222 query: GET /server-status type: http ecs.version: 1.5.0 event.kind: event event.category: net
                              event.dataset: http event.duration: 0.4 event.start: May 23, 2022 @ 20:04:20.222 event.end: May 23, 2022 @ 20:04:20.222 user_agent.original: Go-http-clie
                              network.protocol: http network.community_id: 1:Tb130fcCIc/xodhESHWYFjV+Wt4= network.bytes: 470B network.type: ipv4 network.transport: tcp source.ip: 127
                              source.port: 51101 source.bytes: 109B url.full: http://127.0.0.1/server-status?auto= url.scheme: http url.domain: 127.0.0.1 url.path: /server-status url
                              destination.ip: 127.0.0.1 destination.port: 80 destination.bytes: 361B client.ip: 127.0.0.1 client.port: 51101 client.bytes: 109B agent.version: 7.8.0

May 23, 2022 @ 20:04:10.221   host.name: target1 @timestamp: May 23, 2022 @ 20:04:10.221 agent.name: target1 agent.type: packetbeat agent.version: 7.8.0 agent.hostname: target1
                              agent.ephemeral_id: c39bc2b3-0d8d-451b-b754-c1ec6ac6020b agent.id: 17f60768-4e31-4413-ae13-0f94d41f78f2 user_agent.original: Go-http-client/1.1 event.end:
                              20:04:10.222 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.5 event.start: May 23, 2022 @ 20:04:10.221 http.requ
                              length: 0 http.request.method: get http.request.bytes: 109B http.response.headers.content-length: 158 http.response.headers.content-type: text/plain; char
                              http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 360B http.response.body.bytes: 158B http.version: 1.1 destination.por

May 23, 2022 @ 20:04:00.224   host.name: target1 @timestamp: May 23, 2022 @ 20:04:00.224 client.port: 51099 client.bytes: 109B client.ip: 127.0.0.1 method: get query: GET /server-sta
                              user_agent.original: Go-http-client/1.1 http.request.bytes: 109B http.request.headers.content-length: 0 http.request.method: get http.response.body.bytes
                              http.response.headers.content-length: 158 http.response.headers.content-type: text/plain; charset=ISO-8859-1 http.response.status_phrase: ok http.response
                              http.response.bytes: 360B http.version: 1.1 source.ip: 127.0.0.1 source.port: 51099 source.bytes: 109B type: http status: OK agent.hostname: target1
                              agent.ephemeral_id: c39bc2b3-0d8d-451b-b754-c1ec6ac6020b agent.id: 17f60768-4e31-4413-ae13-0f94d41f78f2 agent.name: target1 agent.type: packetbeat agent.

May 23, 2022 @ 20:03:50.222   host.name: target1 @timestamp: May 23, 2022 @ 20:03:50.222 http.request.bytes: 109B http.request.headers.content-length: 0 http.request.method: get http.
                              http.response.body.bytes: 158B http.response.headers.content-length: 158 http.response.headers.content-type: text/plain; charset=ISO-8859-1 http.response.
                              http.response.status_code: 200 http.version: 1.1 method: get destination.ip: 127.0.0.1 destination.port: 80 destination.bytes: 360B client.port: 51098
```

HTTP REQUEST SIZE MONITOR

- WHEN sum() of http.request.bytes OVER all documents
- IS ABOVE 3500 FOR THE LAST 1 minute

- Checks the availability and response times of web servers.
- If we got too many POST requests it could signal code injection.
- Multiple HTTP requests could signal a possible DDos attacks.



Query: http.request.bytes : * and host.name: "target1"

May 18, 2022 @ 03:25:00.0 → May 18, 2022 @ 03:30:00.0

49,814 hits

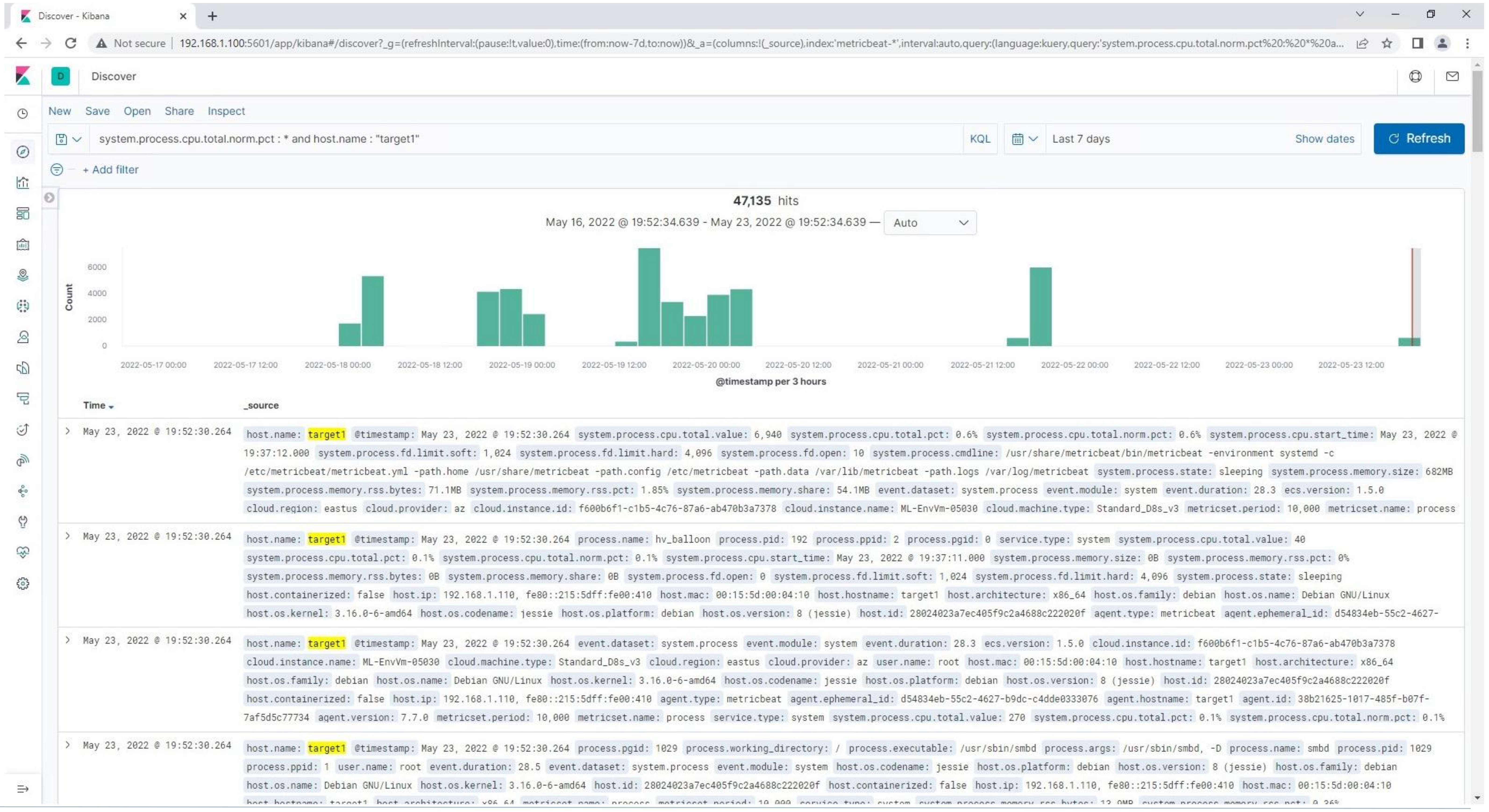
May 18, 2022 @ 03:25:00.000 - May 18, 2022 @ 03:30:00.000

```
May 18, 2022 @ 03:29:59.999   host.name: target1 @timestamp: May 18, 2022 @ 03:29:59.999 query: GET /wordpress/wp-
                              content/tutorials server.bytes: 468B server.ip: 192.168.1.110 server.port: 80
                              http.request.method: get http.request.bytes: 146B http.request.headers.content-length: 0
                              http.response.status_phrase: not found http.response.status_code: 404 http.response.bytes: 468B
```

CPU USAGE MONITOR

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

- Time spent on a certain process.
- Monitors excessive CPU usage which could be a sign that an attacker is running a malicious program.
- User Enumeration could possibly spike CPU usage



```
system.process.cpu.total.norm.pct : * and host.name : "target1"
Last 7 days

47,135 hits
May 16, 2022 @ 19:52:34.639 - May 23, 2022 @ 19:52:34.639 —
```

```
> May 23, 2022 @ 19:52:30.264  host.name: target1 @timestamp: May 23, 2022 @ 19:52:30.264 system.process.cpu.total.value: 6,940 system.process.cpu.total.pct: 0.6% system.process.cpu.total.norm.pct: 0.6% system.process.cpu.start_time: May 23, 2022 @
                               19:37:12.000 system.process.fd.limit.soft: 1,024 system.process.fd.limit.hard: 4,096 system.process.fd.open: 10 system.process.cmdline: /usr/share/metricbeat/bin/metricbeat -environment systemd -c
                               /etc/metricbeat/metricbeat.yml -path.home /usr/share/metricbeat -path.config /etc/metricbeat -path.data /var/lib/metricbeat -path.logs /var/log/metricbeat system.process.state: sleeping system.process.memory.size: 682MB
                               system.process.memory.rss.bytes: 71.1MB system.process.memory.rss.pct: 1.85% system.process.memory.share: 54.1MB event.dataset: system.process event.module: system event.duration: 28.3 ecs.version: 1.5.0
                               cloud.region: eastus cloud.provider: az cloud.instance.id: f600b6f1-c1b5-4c76-87a6-ab470b3a7378 cloud.instance.name: ML-EnvVm-05030 cloud.machine.type: Standard_D8s_v3 metricset.period: 10,000 metricset.name: process

> May 23, 2022 @ 19:52:30.264  host.name: target1 @timestamp: May 23, 2022 @ 19:52:30.264 process.name: hv_balloon process.pid: 192 process.ppid: 2 process.pgid: 0 service.type: system system.process.cpu.total.value: 40
                               system.process.cpu.total.pct: 0.1% system.process.cpu.total.norm.pct: 0.1% system.process.cpu.start_time: May 23, 2022 @ 19:37:11.000 system.process.memory.size: 0B system.process.memory.rss.pct: 0%
                               system.process.memory.rss.bytes: 0B system.process.memory.share: 0B system.process.fd.open: 0 system.process.fd.limit.soft: 1,024 system.process.fd.limit.hard: 4,096 system.process.state: sleeping
                               host.containerized: false host.ip: 192.168.1.110, fe80::215:5dff:fe00:410 host.mac: 00:15:5d:00:04:10 host.hostname: target1 host.architecture: x86_64 host.os.family: debian host.os.name: Debian GNU/Linux
                               host.os.kernel: 3.16.0-6-amd64 host.os.codename: jessie host.os.platform: debian host.os.version: 8 (jessie) host.id: 28024023a7ec405f9c2a4688c222020f agent.type: metricbeat agent.ephemeral_id: d54834eb-55c2-4627-

> May 23, 2022 @ 19:52:30.264  host.name: target1 @timestamp: May 23, 2022 @ 19:52:30.264 event.dataset: system.process event.module: system event.duration: 28.3 ecs.version: 1.5.0 cloud.instance.id: f600b6f1-c1b5-4c76-87a6-ab470b3a7378
                               cloud.instance.name: ML-EnvVm-05030 cloud.machine.type: Standard_D8s_v3 cloud.region: eastus cloud.provider: az user.name: root host.mac: 00:15:5d:00:04:10 host.hostname: target1 host.architecture: x86_64
                               host.os.family: debian host.os.name: Debian GNU/Linux host.os.kernel: 3.16.0-6-amd64 host.os.codename: jessie host.os.platform: debian host.os.version: 8 (jessie) host.id: 28024023a7ec405f9c2a4688c222020f
                               host.containerized: false host.ip: 192.168.1.110, fe80::215:5dff:fe00:410 agent.type: metricbeat agent.ephemeral_id: d54834eb-55c2-4627-b9dc-c4dde0333076 agent.hostname: target1 agent.id: 38b21625-1017-485f-b07f-
                               7af5d5c77734 agent.version: 7.7.0 metricset.period: 10,000 metricset.name: process service.type: system system.process.cpu.total.value: 270 system.process.cpu.total.pct: 0.1% system.process.cpu.total.norm.pct: 0.1%

> May 23, 2022 @ 19:52:30.264  host.name: target1 @timestamp: May 23, 2022 @ 19:52:30.264 process.pgid: 1029 process.working_directory: / process.executable: /usr/sbin/smbd process.args: /usr/sbin/smbd, -D process.name: smbd process.pid: 1029
                               process.ppid: 1 user.name: root event.duration: 28.5 event.dataset: system.process event.module: system host.os.codename: jessie host.os.platform: debian host.os.version: 8 (jessie) host.os.family: debian
                               host.os.name: Debian GNU/Linux host.os.kernel: 3.16.0-6-amd64 host.id: 28024023a7ec405f9c2a4688c222020f host.containerized: false host.ip: 192.168.1.110, fe80::215:5dff:fe00:410 host.mac: 00:15:5d:00:04:10
                               host.hostname: target1 host.architecture: x86_64 metricset.name: process metricset.period: 10,000 service.type: system system.process.memory.rss.bytes: 13.0MB system.process.memory.rss.pct: 0.36%
```

HARDENING

HARDENING AGAINST WEAK PASSWORDS

Create a strong Password policy that has the following requirements:

- Requires a minimum of 10 characters, use one capital letter, one number, and one special character.
- This can be done using Privileged Access Management for linux by
  - nano /etc/pam.d/common-password
  - adding <pam_pwquality.so minlength=9 dcredit=-1 ucredit=-1 lcredit-1 ocredit=-1> to the file
- Requiring passwords to be changed and updated every 60 days.
  - Editing /etc/login.defs to modify password aging controls.
- Multi Factor Authentication.

HARDENING AGAINST MISMANAGED USER PRIVILEGES

Principle of least privilege

- A policy that ensures that users are given only privileges needed to complete tasks.
    - If a subject does not need an access right, the subject should not have that right.
- Also create a password to run root features.
- To implement this policy, we need to run the following command as root
    - sudo visudo
    - and by deleting </usr/bin/python> from the file we will avoid escalation in the future.
- This disallows python from running as root, spawning a shell, effectively mitigating root escalation.

HARDENING AGAINST UNSALTED HASH PASSWORDS ON TARGET 1

- After implementing a strong password policy salt all passwords.
- Update crypto algorithm to SHA-2 (SHA-256) as they are less vulnerable.
- MySQL offers a SHA-2 plugin that is built into the server and built into the *libmysqlclient* client library for activation. This is available only through version 8.0 and up

HARDENING

After hardening against the specific attacks, we recommend also

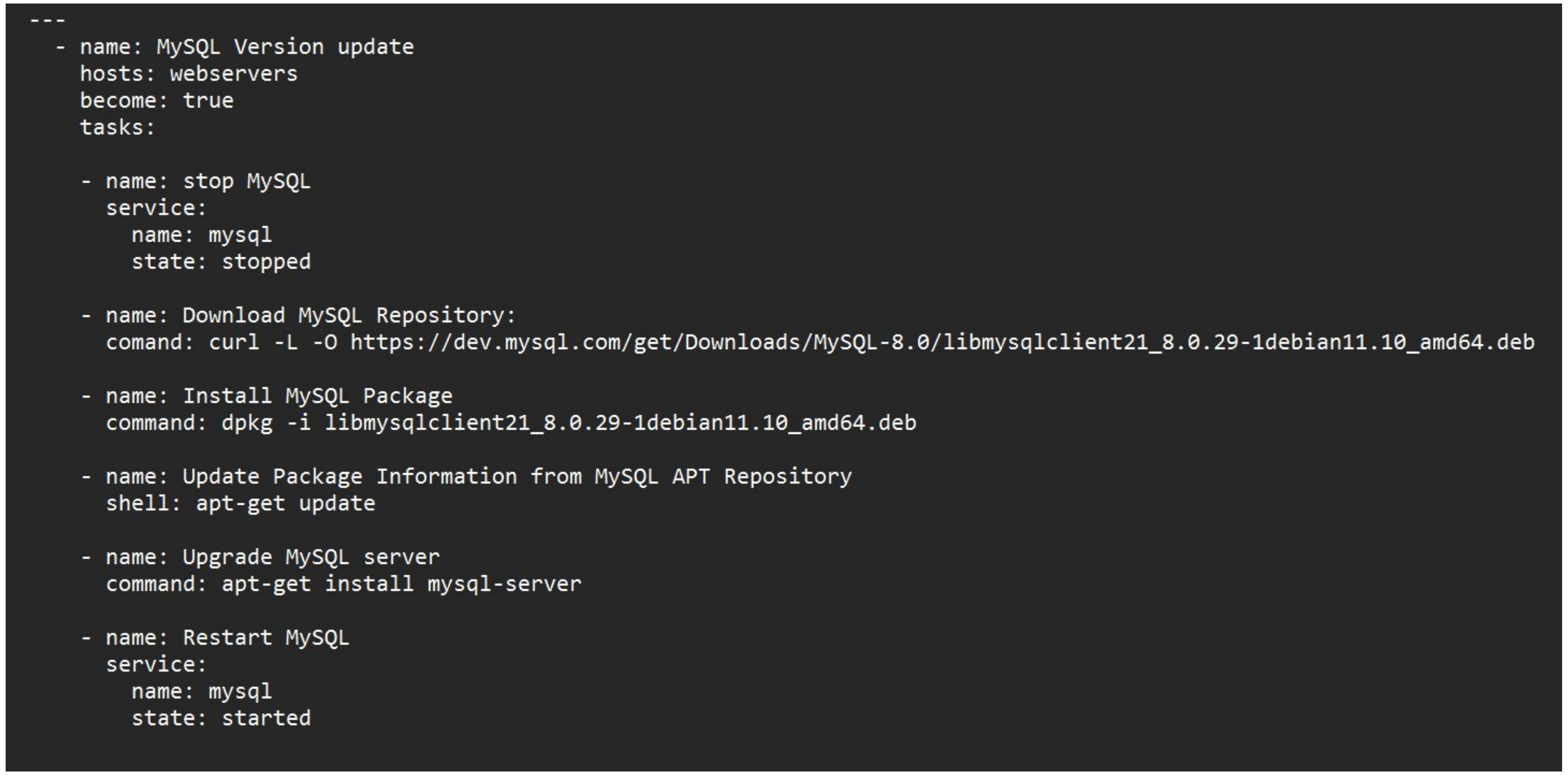
- Updating the firewall policies. Create the a deny all incoming traffic to all and create a whitelist of IP addresses that have access.
- Set up an IDS to monitor ports from port scanning. Snort is a great free source or CrowdStrike Falcon would be a great paid option.
- Set up an alert for any IP trying to access the </var/www/html> directory.
- Create educational programs to make end users aware of the dangers of online threats. IT team can hold quarterly or biannual training meetings to teach. IT team can also send emails about the dangers of online threat in a educational pamphlet format.

IMPLEMENTING PATCHES

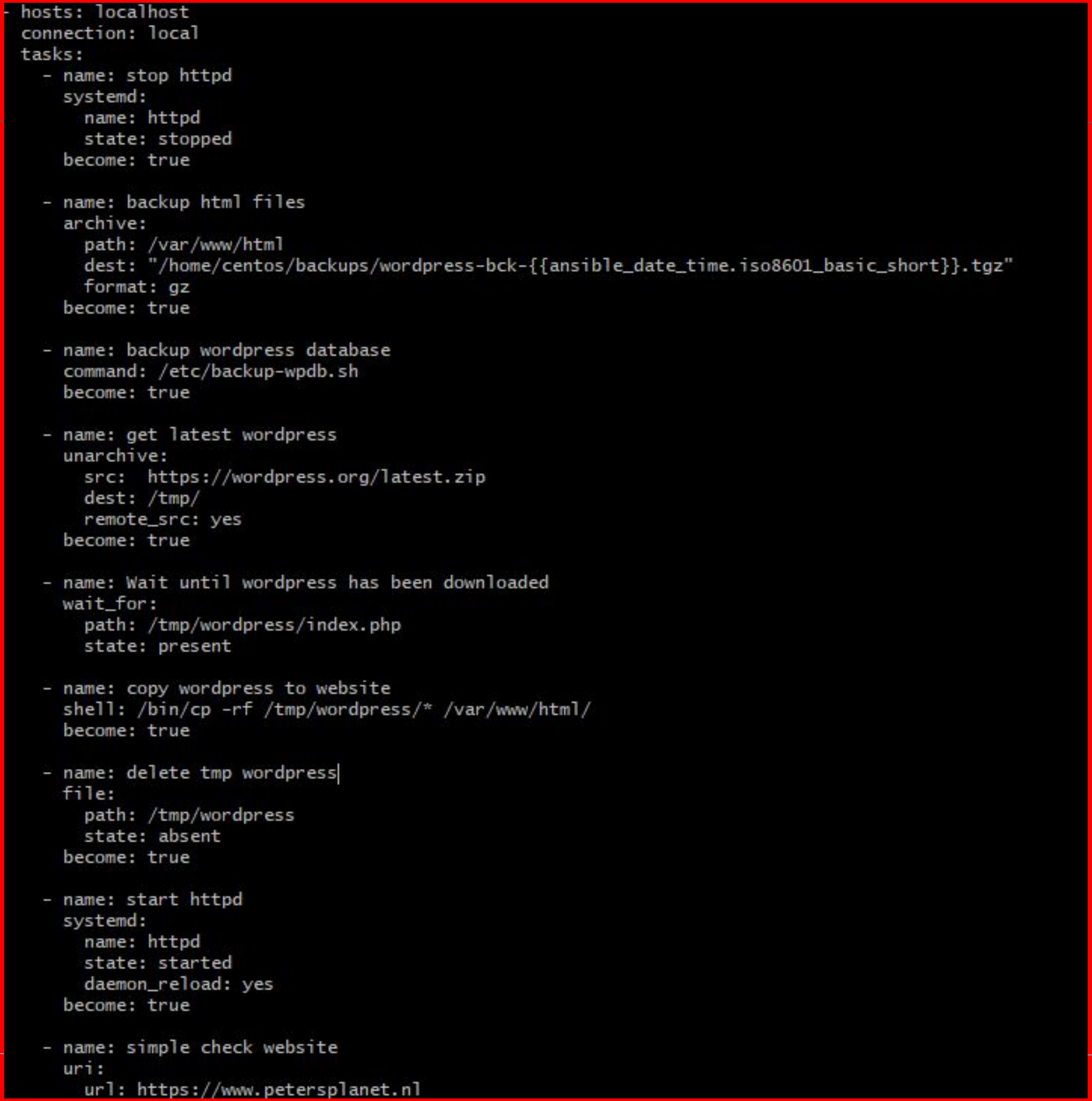
IMPLEMENTING PATCHES WITH ANSIBLE

Playbook Overview

- Upgrade MySQl and WordPress the the most current versions.



```
---
  - name: MySQL Version update
    hosts: webservers
    become: true
    tasks:

    - name: stop MySQL
      service:
        name: mysql
        state: stopped

    - name: Download MySQL Repository:
      comand: curl -L -O https://dev.mysql.com/get/Downloads/MySQL-8.0/libmysqlclient21_8.0.29-1debian11.10_amd64.deb

    - name: Install MySQL Package
      command: dpkg -i libmysqlclient21_8.0.29-1debian11.10_amd64.deb

    - name: Update Package Information from MySQL APT Repository
      shell: apt-get update

    - name: Upgrade MySQL server
      command: apt-get install mysql-server

    - name: Restart MySQL
      service:
        name: mysql
        state: started
```



```
- hosts: localhost
  connection: local
  tasks:
    - name: stop httpd
      systemd:
        name: httpd
        state: stopped
      become: true

    - name: backup html files
      archive:
        path: /var/www/html
        dest: "/home/centos/backups/wordpress-bck-{{ansible_date_time.iso8601_basic_short}}.tgz"
        format: gz
      become: true

    - name: backup wordpress database
      command: /etc/backup-wpdb.sh
      become: true

    - name: get latest wordpress
      unarchive:
        src:  https://wordpress.org/latest.zip
        dest: /tmp/
        remote_src: yes
      become: true

    - name: Wait until wordpress has been downloaded
      wait_for:
        path: /tmp/wordpress/index.php
        state: present

    - name: copy wordpress to website
      shell: /bin/cp -rf /tmp/wordpress/* /var/www/html/
      become: true

    - name: delete tmp wordpress
      file:
        path: /tmp/wordpress
        state: absent
      become: true

    - name: start httpd
      systemd:
        name: httpd
        state: started
        daemon_reload: yes
      become: true

    - name: simple check website
      uri:
        url: https://www.petersplanet.nl
```

04 WINS
70
00 WINS
Lew Kang
Kris
FRIENDSHIP
?