MUNI
FI

Cyber Threat Management – Seminar

PA211 Advanced Topics of Cyber Security

October 4, 2022

Lukáš Sadlek, Jan Vykopal, and Pavel Čeleda

Goals of this tutorial

- Become **acquainted** with:
  - **SIEM features** provided by Elastic Security (**alerts, detection rules**)
  - **Ingesting data** to Elasticsearch from Beats
  - Data analysis for cyber **threat discovery**

Prerequisites – I

1. Run **`pa211_setup`** command on a school computer.
2. Change your working directory to the clone of repository from the previous week

   https://gitlab.fi.muni.cz/cybersec/pa211/management.git
3. Run **`git pull`**.
4. Change directory to **`siem`**. This directory should contain **`Vagrantfile`**.
5. Run **`vagrant up`**. **Remember the port** number used for **SSH** (usually 2222).

   We will **use it** during the seminar.
6. We will use only one **host** named **`elk`**.

MUNI FI

Prerequisites – II

- Use the **port forwarding** command to access services from your host:
  1. `vagrant ssh elk -- -L 5601:localhost:5601`
- Verify that you can **access** `http://localhost:5601`
- Log into the **Kibana user interface** using credentials `elastic:elastic`

MUNI FI

Important notes

- **Elasticsearch** and **Kibana** containers restart **automatically**
- If you experience **issues**
  - Run `docker container ls -a`
  - If containers are up **at least one minute**, you can **repeat an action** in Kibana UI
  - If containers are exited and do **not restart**, run `docker start <container_id>`
- **Do not** use reload in your **browser**, but refresh **in Kibana UI**
- Kibana provides an option to **save a created panel**
- **Do not destroy** the virtual machine

MUNI FI

Troubleshooting – I

- **Destroy** and **create** a virtual machine
  - `vagrant destroy <machine_name> -f`
  - `Vagrant up <machine_name>`
- **Rerun** ansible tasks, if ansible script **failed**
  - `vagrant provision <machine_name>`
- **Start all** containers
  - `sudo docker start $(sudo docker ps -aq)`
- **List all** (not only running) containers
  - `sudo docker container ls -a`

Troubleshooting – II

- List **open ports** on device
  - `sudo netstat -tulpn`
- **Check logs** of a specific **container** for issues
  - `sudo docker logs <container_id>`
- The first tasks **does not** contain solutions
  - A solution is **correct**, if it **accomplishes** the specified tasks
- Do not look at **the consequent slide**
  - It can contain **hints**

MUNI FI

Elastic Security

Elastic Security

- Provides SIEM **features**
- **Beats** or **Logstash pipeline** to ingest data
- Threat **detection** and **hunting**
- **Security data** analysis
- **Demonstration** of user interface and data sources

MUNI FI

Task 1 – Auditbeat – I

- Try to configure **`elk` virtual machine** so that you will be able to obtain data from **Auditbeat**. Auditbeat collects **audit data** about the activities of **users** and **processes** on the system. In the **Kibana menu**, choose Security – Overview – Add data with Beats – Auditbeat. In **Getting started** tutorial, choose **DEB**, and we will **partially** follow these steps on the **`elk` host**.
- **Accomplish step 1** on your `elk` host.
- Continue with the **following slides**.

Task 1 – Auditbeat – II

- **Step 2** will be more **complicated** because we use **HTTPS**
- For **editing files**, you can use `sudo nano auditbeat.yml`
- `auditbeat.yml` contains **some content**
  - There are sections: **Kibana** and **Elasticsearch output**
  - `<kibana_url>` is `"localhost:5601"`,
  - `<es_url>` is `"https://localhost:9200"`,
  - `<password>` is `"elastic"`
- Use the **https** protocol to connect to the **`elasticsearch`** container
- **Uncomment the line** about protocol in the `auditbeat.yml` file

MUNI FI

Task 1 – Auditbeat – III

- Add **certificate information** to `auditbeat.yml` with the **right indent**

```
ssl:
  certificate_authorities: ["elasticsearch-ca.pem"]
  verification_mode: "certificate"
```

- **Do not** copy but write it
- Key `ssl` is on the **same level** as `password` in **Elasticsearch output** section
- It is necessary to **add** a **certificate** to `/etc/auditbeat`
- Create an **empty file** **`elasticsearch-ca.pem`** in the folder (with sudo)
- Copy to the file **content** of the `.pem` file from the **study materials**

MUNI FI

Task 1 – Auditbeat – IV

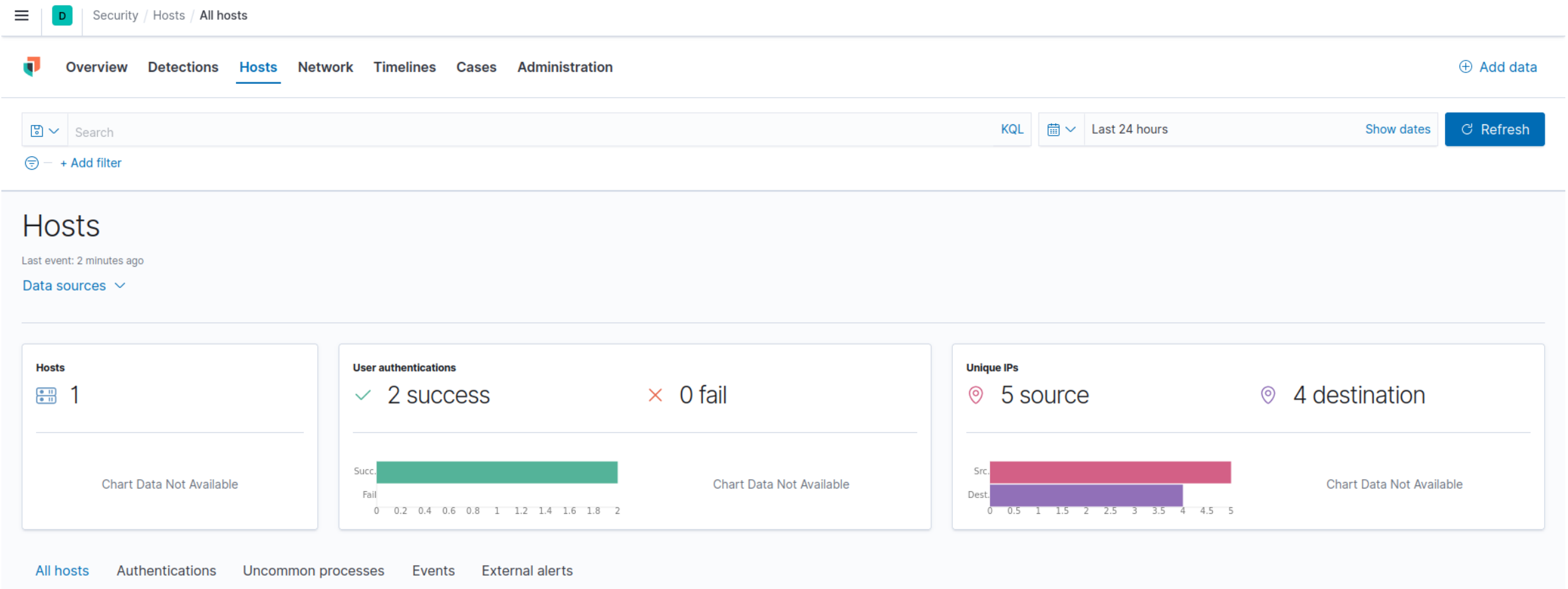
- Continue with **step 3** from elastic **documentation**:
  - `sudo auditbeat setup`
  - `sudo service auditbeat start`
- Wait for **a minute** and **look for data** in Kibana in Security – Overview – Host events at the bottom of the page
- If no data, run on **`elk` host:** `sudo auditbeat -e -d "*"`
- Let it run **for a minute, and then press** `Ctrl + C` to **stop** it

MUNI FI

Task 1 – Auditbeat – V

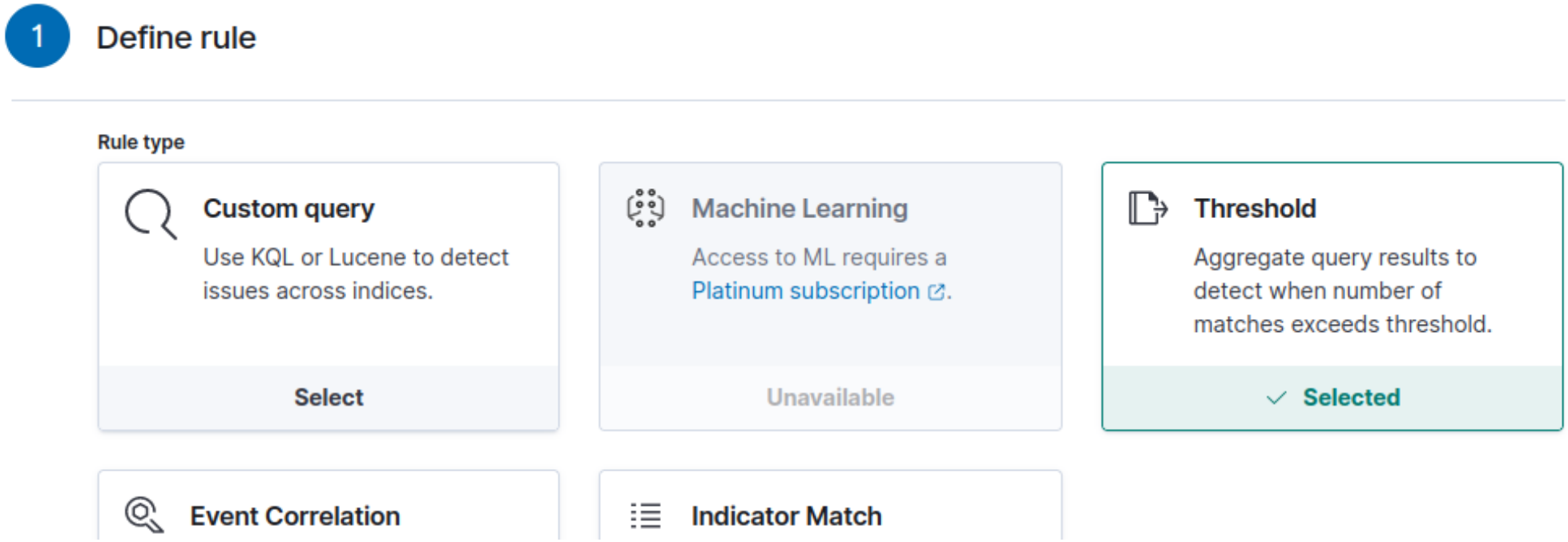
- You should see **some data** in Security – Overview – Host events and Security – Hosts
- The following slide contains an **example output**
- In **Dashboards**, look at some of the **auditbeat dashboards**
- Then use **`[Auditbeat System] Login Dashboard ECS`**
- It contains **hosts, logins, processes**, and other information

Task 1 – Auditbeat – VI



Task 2 – detection rule – I

- Create a **threshold rule** detecting **more than two unsuccessful** login attempts
- **Create a rule** in Security – Detections – Manage detection rules – Create your own rules



MUNI FI

Task 2 – detection rule – II

- Now, you should see the "**Define rule**" part of the form.
- Create a threshold-based detection rule called "**many unsuccessful login attempts**"
- It will be applied when more than **two unsuccessful** login attempts are captured in the data f or **a specific** username
- Use **only auditbeat-*** index pattern**.**
- It is necessary to fill in a **custom query** that will obtain only relevant data and determine the **name of** an **attribute** upon which the threshold will be applied
- Try to create the custom query and the threshold based on exploring **properties and values** from the **login dashboard** before switching to the following slide (see also [1])

MUNI FI

Task 2 – detection rule – III

- In the **login dashboard**, there are
  - **`event.outcome`** with values: `success` and `failure`
  - `user.name` that denotes **username**
- If you expand one of the login **rows** in the **login events table**
  - The **attribute** has name `event.action`
  - The name of **action** is `"user_login"`
- Custom **query field** can contain
  - `event.outcome: "failure" and event.action: "user_login"`
- **Group by** part can contain
  - `user.name >= 3 (threshold)`

MUNI FI

Task 2 – detection rule – IV

- **"About rule"** part of the form
  - Write some **description**
  - Assign **LOW severity** and default risk **score** of **25%**
  - In **Advanced** settings, use the MITRE ATT&CK **Credential Access** tactic
- **"Schedule rule"** part
  - Run every **5 minutes** and with **1 minute look-back** time
- The rule should **not perform** any actions
- Create and **activate** the rule
- **Check** that it was created **successfully**

MUNI FI

Task 3 – alert – I

- We need some **data** to create an **alert** based on the detection rule
- Run on your **local host** (not on the `elk` machine)
  - `ssh -p 2222 <your_first_name>@localhost`
  - replace the **port number** to another, if your **ssh** on the virtual machine was **not set to 2222**
- Try to **authenticate** on this **non-existing** account at least **five times**
- Go to Security - Hosts and **check** that auditbeat found some **login failures**
- If not, **obtain data**
  - `sudo auditbeat -e -d "*"` on **`elk` host**,
  - exit with `Ctrl + C` after **one minute**

MUNI FI

Task 3 – alert – II

- Go to Security – Detection – **Manage detection rules**
  - Click on "**many unsuccessful login attempts**" rule
  - **Alerts** can be found **at the bottom** of the page
  - **Check** whether it generated **some alert**
  - Otherwise, **wait** for the **next run** of the detection rule
  - Always use the **Refresh** button **instead** of reloading in the browser
  - Look also to the **[Auditbeat System] Login Dashboard ECS** in dashboards

MUNI FI

Task 4 – add default rules – I

- Go to Security – Detections – **Manage detection rules**
- Add all Elastic **prebuilt rules**
- **Tags** for these rules describe
  - **Platforms** where the rule is **applicable**, such as Windows tag
  - Relationship to **MITRE ATT&CK**, e.g., Lateral Movement or Defense Evasion **tactic**
- **Choose**
  - One rule related to ATT&CK **privilege escalation** tactic
  - One rule for **defense evasion** tactic
  - **Do not** use Windows-specific rules, `elk` host has **Debian** OS
- **Activate** the two rules and **check** successful execution in **Manage detection rules**

MUNI FI

Task 4 – add default rules – II

– **Repository** for rules [1] and their **coverage** of MITRE ATT&CK [2]

Rules | Rule Monitoring | Exception Lists

All rules

Updated 2 seconds ago

e.g. rule name | Tags | Elastic rules (546) | Custom rules (1)

Showing 547 rules | Selected 0 rules | Bulk actions | Refresh | Refresh settings

Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated
Suspicious Child Process of Adobe Acrobat Reader Update Service	73	High	2 minutes ago	succeeded	Oct 3, 2022 @ 08:40:10.635	1	Elastic, Host, macOS, See all	✓
Potential Privacy Control Bypass via Localhost Secure Copy	73	High	2 minutes ago	succeeded	Oct 3, 2022 @ 08:40:39.882	1	Defense Evasion, Elastic, Host, See all	✓
many unsuccessful login attempts	25	Low	1 minute ago	succeeded	Oct 3, 2022 @ 08:26:05.877	1	—	✓
Unusual Child Process from a System Virtual Process	73	High	—	—	Oct 3, 2022 @ 08:38:14.053	3	Defense Evasion, Elastic, Host, See all	✗
Suspicious DLL Loaded for Persistence or Privilege Escalation	73	High	—	—	Oct 3, 2022 @ 08:38:14.247	1	Elastic, Host, Persistence, See all	✗

MUNI FI

Optional: Task 5 – suspicious traffic – I

IP flow dataset with index pattern `threats-2019-03-19` contains suspicious traffic with a **sudden spike**. **More** IP addresses than **usually** communicated with **one web server**. It may be a sign of a **denial-of-service** attempt. The traffic is stored as **bidirectional flow** where the **destination** is also the **source** of communication **in the opposite** direction. Create a new **Lens dashboard panel** and set your time range to **last five years**.

Optional: Task 5 – suspicious traffic – II

a) Find the IP address of the **web server**. It is an **IP address** that communicated with **the highest number** of IP addresses.

b) Determine **IP addresses** that communicated with the webserver **approximately** at the same time during the **sudden spike**.

c) Determine the **approximate time range** when the sudden spike appeared. Use **10 seconds long** time intervals for timestamps, if needed.

Solution 5 a)

- `9.66.11.14` communicated with the **highest number** of IP addresses

Data table

Top values of destinationIPv4Address	Top values of sourceIPv4Address	Count of records
4.122.55.3	9.66.11.13	324
4.122.55.3	9.66.11.12	10
9.66.11.12	4.122.55.5	67
9.66.11.13	4.122.55.5	25
9.66.11.13	4.122.55.3	10
9.66.11.14	4.122.55.5	9
9.66.11.14	52.138.148.89	3
52.138.148.89	9.66.11.14	9
104.103.90.39	9.66.11.14	9
4.122.55.5	9.66.11.12	3
4.122.55.5	9.66.11.14	1
20.42.24.50	9.66.11.14	2
65.55.252.93	9.66.11.14	2
52.138.216.83	9.66.11.14	1
192.5.6.30	9.66.11.13	1

MUNI FI

5 b) c)

- **IP addresses**
  - 65.55.252.93
  - 20.42.24.50
  - 52.138.148.89
  - 104.103.90.39
- **Time range**
  - 15:58:40 – 15:59:00

Data table

Top values of destinationIPv4...	Top values of sourceIPv4Addr...	timestamp per 10 seconds	Count of records
4.122.55.3	9.66.11.13	15:58:20	2
4.122.55.3	9.66.11.13	15:58:30	2
4.122.55.3	9.66.11.13	15:58:40	4
65.55.252.93	9.66.11.14	15:58:40	1
4.122.55.3	9.66.11.13	15:58:50	0
20.42.24.50	9.66.11.14	15:58:50	1
65.55.252.93	9.66.11.14	15:58:50	0
4.122.55.3	9.66.11.13	15:59:00	5
9.66.11.14	52.138.148.89	15:59:00	3
52.138.148.89	9.66.11.14	15:59:00	9
104.103.90.39	9.66.11.14	15:59:00	9
20.42.24.50	9.66.11.14	15:59:00	1
65.55.252.93	9.66.11.14	15:59:00	1
4.122.55.3	9.66.11.13	15:59:10	0
4.122.55.3	9.66.11.13	15:59:20	0
4.122.55.3	9.66.11.13	15:59:30	0
4.122.55.3	9.66.11.13	15:59:40	0
4.122.55.3	9.66.11.13	15:59:50	4

MUNI FI

Homework 1

- Your task is to **analyze** packets in **Kibana**
- You can obtain **15 points** (¼ of the total homework points)
- **Assignment** can be found in this **MS Form** [1]
- **Answers** are submitted using the same **MS Form** at [1]
  - You can submit more than one answer, we will mark the last one.
- **Deadline: October 18, 10.00 (no extension)**
- The virtual machine uses **6 GB** of **RAM**

Homework 1 – setup

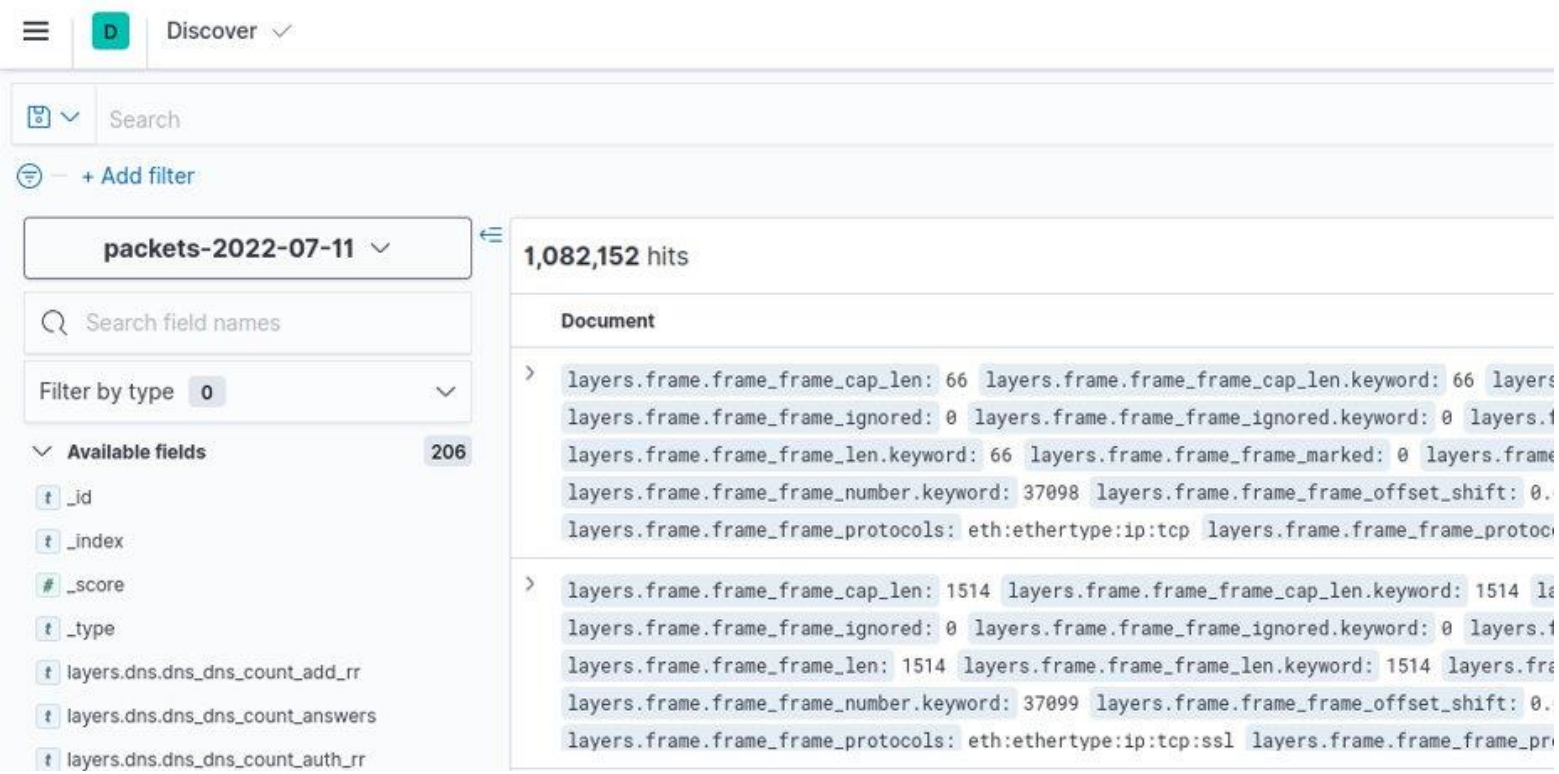
1. Run **`pa211_setup`** command on a school computer.
2. Use sandbox and repository from this week: **`https://gitlab.fi.muni.cz/cybersec/pa211/management.git`**
3. Run **`git pull`**.
4. Change working directory to **`hw1`**. This directory contains **`Vagrantfile`**.
5. Run **`vagrant up`**. We will use only one **host** named **`elk`**.
6. Use **port forwarding** to access `http://localhost:5601` from your **host**:

   `vagrant ssh elk -- -L 5601:localhost:5601` (do **not exit** `elk` host while solving HW)

MUNI FI

Homework 1 – count of documents

– **Check** the **count** of documents (1,082,152) in the **Discover** section



MUNI FI

Homework 1 – notes

- Use **`vagrant halt`** to power off the virtual machine
- It will **not destroy** it and its data
- The machine can be **started** using **`vagrant up`**
- **Ignore warning** "Your data is not secure"
  - The elasticsearch container **is not** configured to use **HTTPS**
- Contact person for this homework: Lukáš Sadlek <sadlek@mail.muni.cz>

MUNI FI

How was it today?

Please fill in an **anonymous** exit ticket:

https://muni.cz/go/pa211-22-04

MUNI
FI