Threat Hunting Lab Part 1 Setup : ELK as a docker image in an Ubuntu VM

Configure ELK on Ubuntu 20.04 LTS (Desktop) system : You can run this as a VM in VMware WorkStation/Fusion or Oracle VirtualBox

* 1. Install Ubuntu 20.04 (18.04 could work too)
     1. Get ISO from Ubuntu site (https://ubuntu.com/download/desktop)
     2. Use 4 or 8 GB of RAM, 2 or 4 CPU for your VM. 25 GB of Disk or more.
     3. Use NAT for your NIC or Bridge if you want to share in your LAN
     4. Update your os and reboot
  2. Install some dependencies
  3. Install Docker on Ubuntu
  4. Get this lab zip file that contain docker compose script and logs
     1. Elastic stack 7.6.0 (this is the one I used but newer version could work too)
  5. Confirmed Kibana on your Ubuntu run and reachable (5601 port in your browser)
  6. Download sample logs from SANS DeepBlueCLI github repo or the link provided
  7. Ingest event log (evtx) in Elastic
  8. Verify the logs are imported in Kibana

## Detailed procedure in Ubuntu

-1 Once Ubuntu installed, make sure to apply updates

sudo apt update

sudo apt install net-tools

ifconfig # take note of your IP, you will need it

-2 install pip3 so you can install some python libraries you will need

sudo apt install python3-pip

-3 install pycharm community

Use Ubuntu software to get it. Then add it to favorites

-4 install EvtxToElk python library so you can import the Windows events logs from the labs into Elastic

Pip3 install evtxtoelk

-5 install curl

sudo apt install curl

-6 Install Docker in Ubuntu (reference : https://phoenixnap.com/kb/install-docker-on-ubuntu-20-04)

sudo apt-get install apt-transport-https ca-certificates curl software-properties-common

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add –

sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb\_release -cs) stable”

sudo apt update

sudo apt-get install docker-ce

docker –version

sudo systemctl start docker

sudo systemctl enable docker

sudo systemctl status docker

sudo apt install docker-compose

-7 Create docker compose file for Elastic and Kibana and execute it

Get the docker compose file from : https://github.com/girdav01/utils/blob/main/docker-compose.yml

Create directory elastic in \home

Mkdir elastic

Copy the compose file (docker-compose.yml) in elastic directory

Get in elastic directory

cd elastic

start it

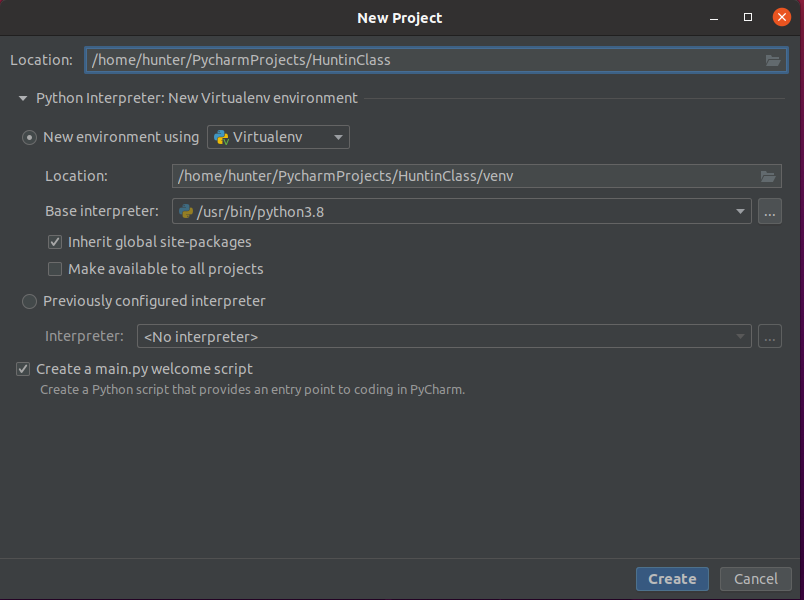
sudo docker-compose up

Test elastic by opening a browser : <http://localhost:9200>

Test Kibana by opening a browser : <http://localhost:5601>

You can also use the ip instead of localhost

-8 Open PyCharm and create a new project HuntClass so we can import the Windows event logs in Elastic



Create a new python file (importEvtxFilesToElastic.py) in your project and copy code from <https://github.com/girdav01/utils/blob/main/ImportEvtxFilesToElastic.py>

Download Sans intitute training logs

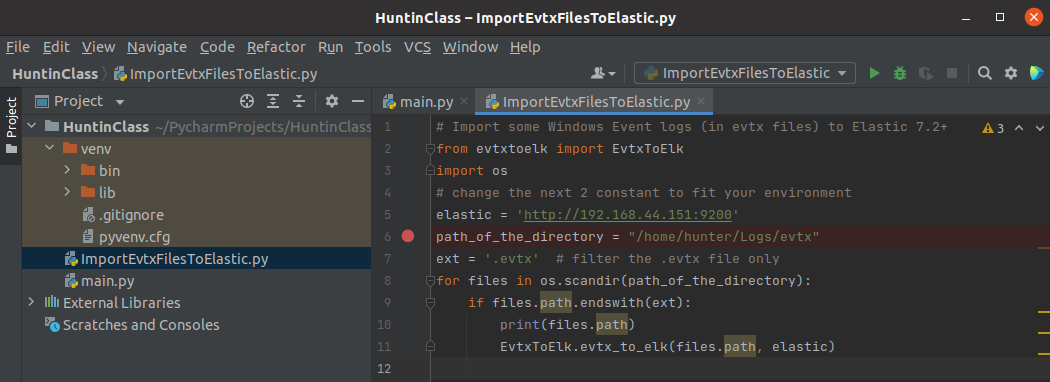
<https://trendmicro-my.sharepoint.com/:u:/p/david_girard/ER4TrLqSWStAvf-S1yycDFIBlYEqUL-IzB6bfOhoINDcyQ?e=849cc9>

create a Logs directory under /home

In download folder open DeepBlueCLI-Master.zip with archive manager and extract evtx folder to Logs folder you just created.

*Note that you might want to see the powerShell and python files in this zip file if you are interested after this workshop.*

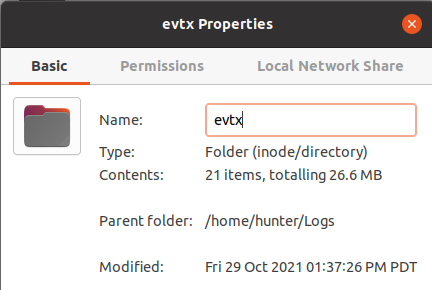
In PyCharm, change elastic and path\_of\_the\_directory constant. The path must have your user in it. Like in my example here my user is hunter so the logs are in /home/hunter/Logs/evtx



Run it 

Importing 26K logs will take around 5 minutes (coffee break).

If you get errors on path, check the Logs\evtx directory. It is the Parent Folder name you need to pass



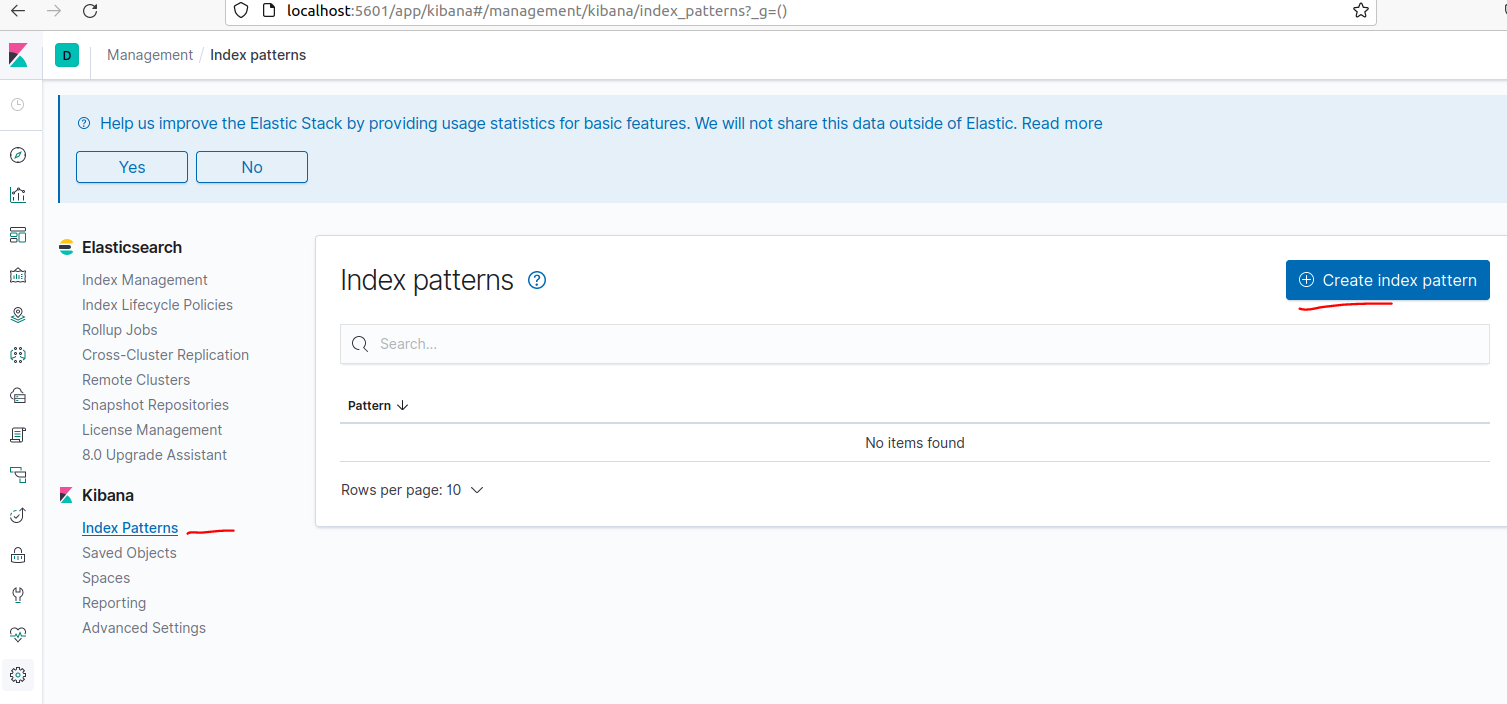
Make sure you ran step 4 at the beginning and EvtxToElk is properly installed. If not ask the instructor. Or add it in pyCharm project if you know how to.

Run again!

Next step you must create index in Kibana (<http://your-Ip:5601>)

Go in Management 

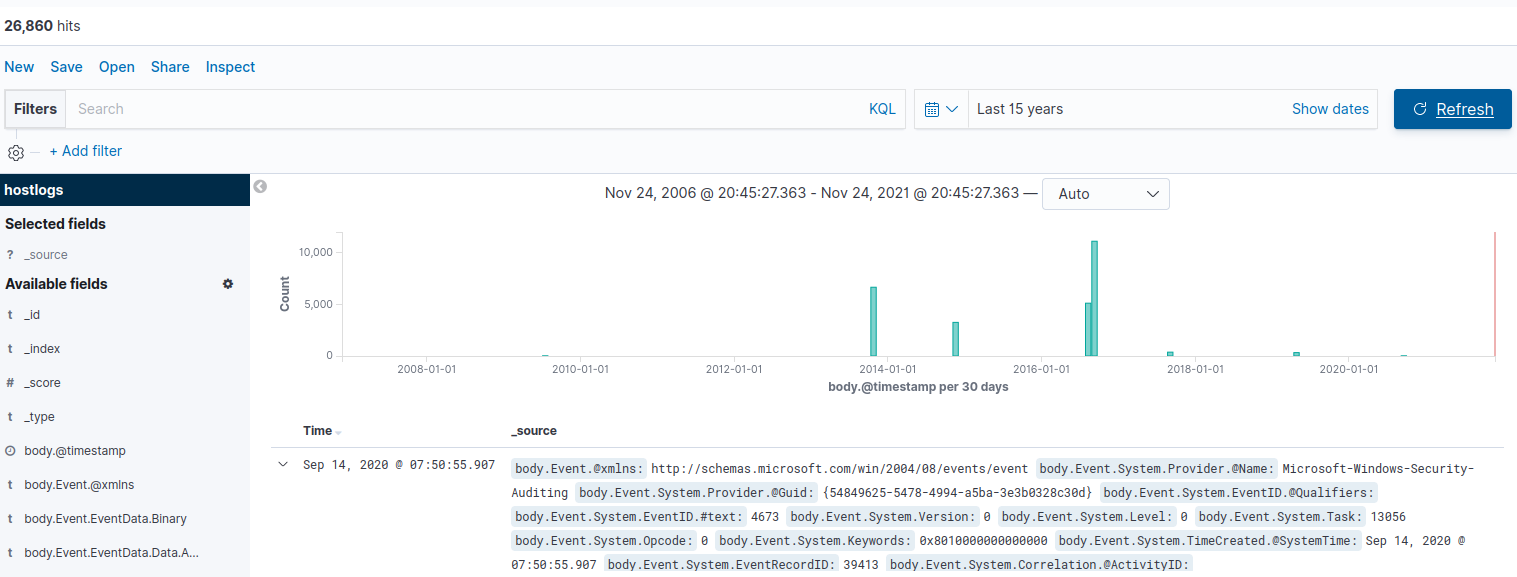
Select Index Patterns, then Create index pattern



Name it hostlogs, click next

Pick [body.@timestamp](mailto:body.@timestamp) as the Time Filter field name and click on create index pattern

Now go to Discover Select last 15 years to be sure to get all logs, you should have 26 860 hits (logs)



Bravo now you can start hunting!