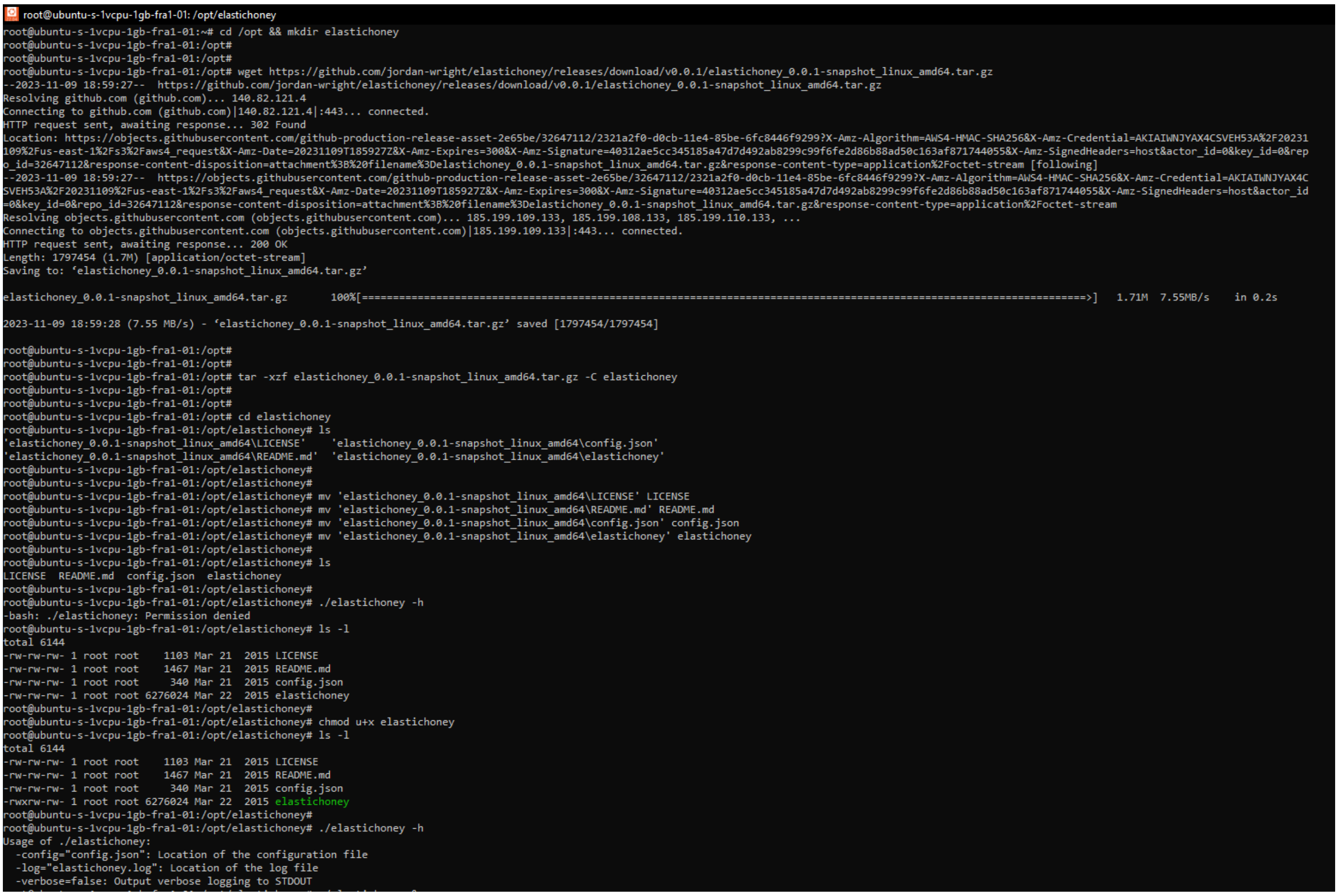
# CS437 LAB 2 Report

## Uğur Öztunç 28176

### Installing and deploying *Elastichoney*:

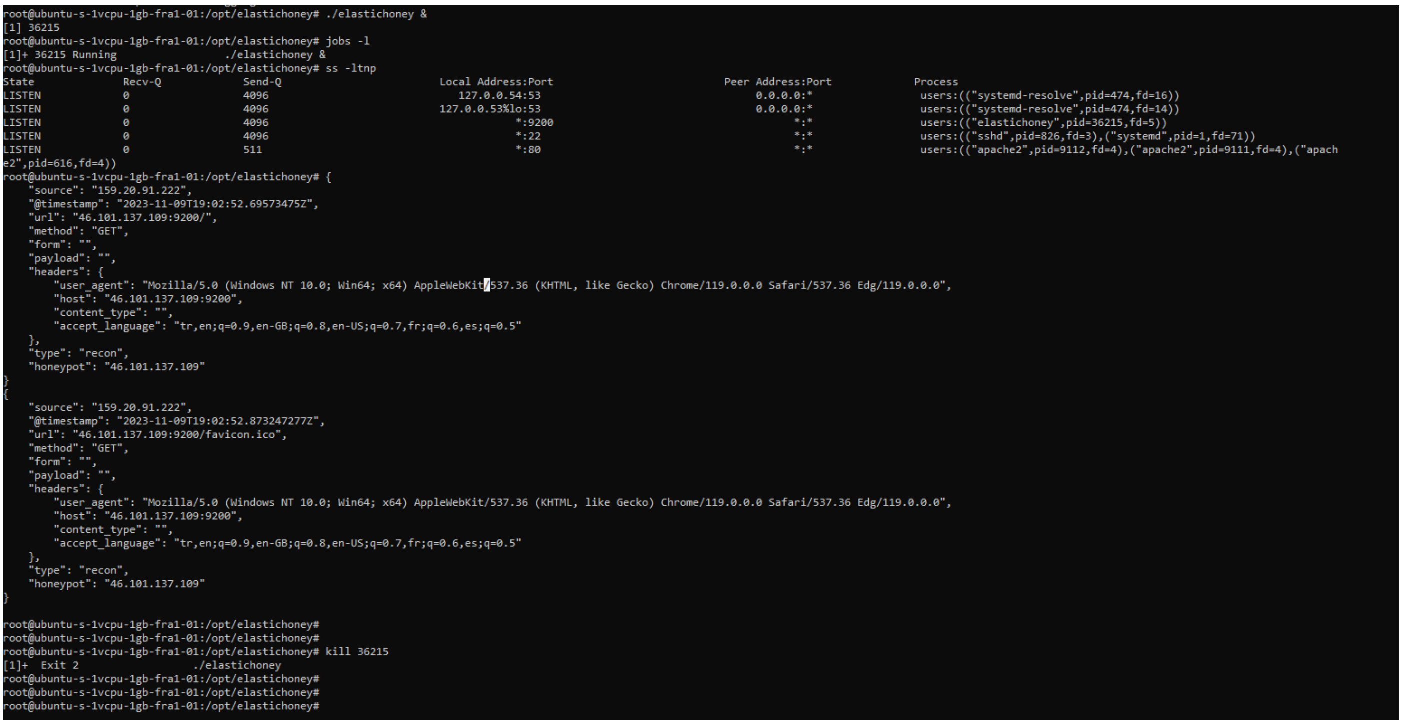
To install the Elastichoney, I first created a new directory in '/opt/' named 'elastichoney'. Then, by using wget command, along with the release link for my OS that I obtained from Github repo, I've downloaded the program as an archive. Then I used tar command to extract the archive to the directory that I've created. I could not find out the reason or rationale but all files are got extracted from archive with archive's name added at the beginning of them. Therefore, I've manually changed all files' names to their normal names by using mv command. Then I tried to run the executable file of elastichoney, but it did not run. Then I noticed that there is no permission to execute it. I added the permission to execute it by using chmod command then managed to run it with -h option. Here is the process:



```
root@ubuntu-s-1vcpu-1gb-fra1-01: /opt/elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:~# cd /opt && mkdir elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt# wget https://github.com/jordan-wright/elastichoney/releases/download/v0.0.1/elastichoney_0.0.1-snapshot_linux_amd64.tar.gz
--2023-11-09 18:59:27--  https://github.com/jordan-wright/elastichoney/releases/download/v0.0.1/elastichoney_0.0.1-snapshot_linux_amd64.tar.gz
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/32647112/2321a2f0-d0cb-11e4-85be-6fc8446f9299?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20231
109%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20231109T185927Z&X-Amz-Expires=300&X-Amz-Signature=40312ae5cc345185a47d7d492ab8299c99f6fe2d86b88ad50c163af871744055&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&rep
o_id=32647112&response-content-disposition=attachment%3B%20filename%3Delastichoney_0.0.1-snapshot_linux_amd64.tar.gz&response-content-type=application%2Foctet-stream [following]
--2023-11-09 18:59:27--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/32647112/2321a2f0-d0cb-11e4-85be-6fc8446f9299?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4C
SVEH53A%2F20231109%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20231109T185927Z&X-Amz-Expires=300&X-Amz-Signature=40312ae5cc345185a47d7d492ab8299c99f6fe2d86b88ad50c163af871744055&X-Amz-SignedHeaders=host&actor_id
=0&key_id=0&repo_id=32647112&response-content-disposition=attachment%3B%20filename%3Delastichoney_0.0.1-snapshot_linux_amd64.tar.gz&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.110.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1797454 (1.7M) [application/octet-stream]
Saving to: 'elastichoney_0.0.1-snapshot_linux_amd64.tar.gz'

elastichoney_0.0.1-snapshot_linux_amd64.tar.gz       100%[===================================================================================================================>]   1.71M  7.55MB/s    in 0.2s

2023-11-09 18:59:28 (7.55 MB/s) - 'elastichoney_0.0.1-snapshot_linux_amd64.tar.gz' saved [1797454/1797454]

root@ubuntu-s-1vcpu-1gb-fra1-01:/opt#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt# tar -xzf elastichoney_0.0.1-snapshot_linux_amd64.tar.gz -C elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt# cd elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# ls
'elastichoney_0.0.1-snapshot_linux_amd64\LICENSE'    'elastichoney_0.0.1-snapshot_linux_amd64\config.json'
'elastichoney_0.0.1-snapshot_linux_amd64\README.md'  'elastichoney_0.0.1-snapshot_linux_amd64\elastichoney'
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# mv 'elastichoney_0.0.1-snapshot_linux_amd64\LICENSE' LICENSE
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# mv 'elastichoney_0.0.1-snapshot_linux_amd64\README.md' README.md
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# mv 'elastichoney_0.0.1-snapshot_linux_amd64\config.json' config.json
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# mv 'elastichoney_0.0.1-snapshot_linux_amd64\elastichoney' elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# ls
LICENSE  README.md  config.json  elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# ./elastichoney -h
-bash: ./elastichoney: Permission denied
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# ls -l
total 6144
-rw-rw-rw- 1 root root    1103 Mar 21  2015 LICENSE
-rw-rw-rw- 1 root root    1467 Mar 21  2015 README.md
-rw-rw-rw- 1 root root     340 Mar 21  2015 config.json
-rw-rw-rw- 1 root root 6276024 Mar 22  2015 elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# chmod u+x elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# ls -l
total 6144
-rw-rw-rw- 1 root root    1103 Mar 21  2015 LICENSE
-rw-rw-rw- 1 root root    1467 Mar 21  2015 README.md
-rw-rw-rw- 1 root root     340 Mar 21  2015 config.json
-rwxrw-rw- 1 root root 6276024 Mar 22  2015 elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# ./elastichoney -h
Usage of ./elastichoney:
  -config="config.json": Location of the configuration file
  -log="elastichoney.log": Location of the log file
  -verbose=false: Output verbose logging to STDOUT
```

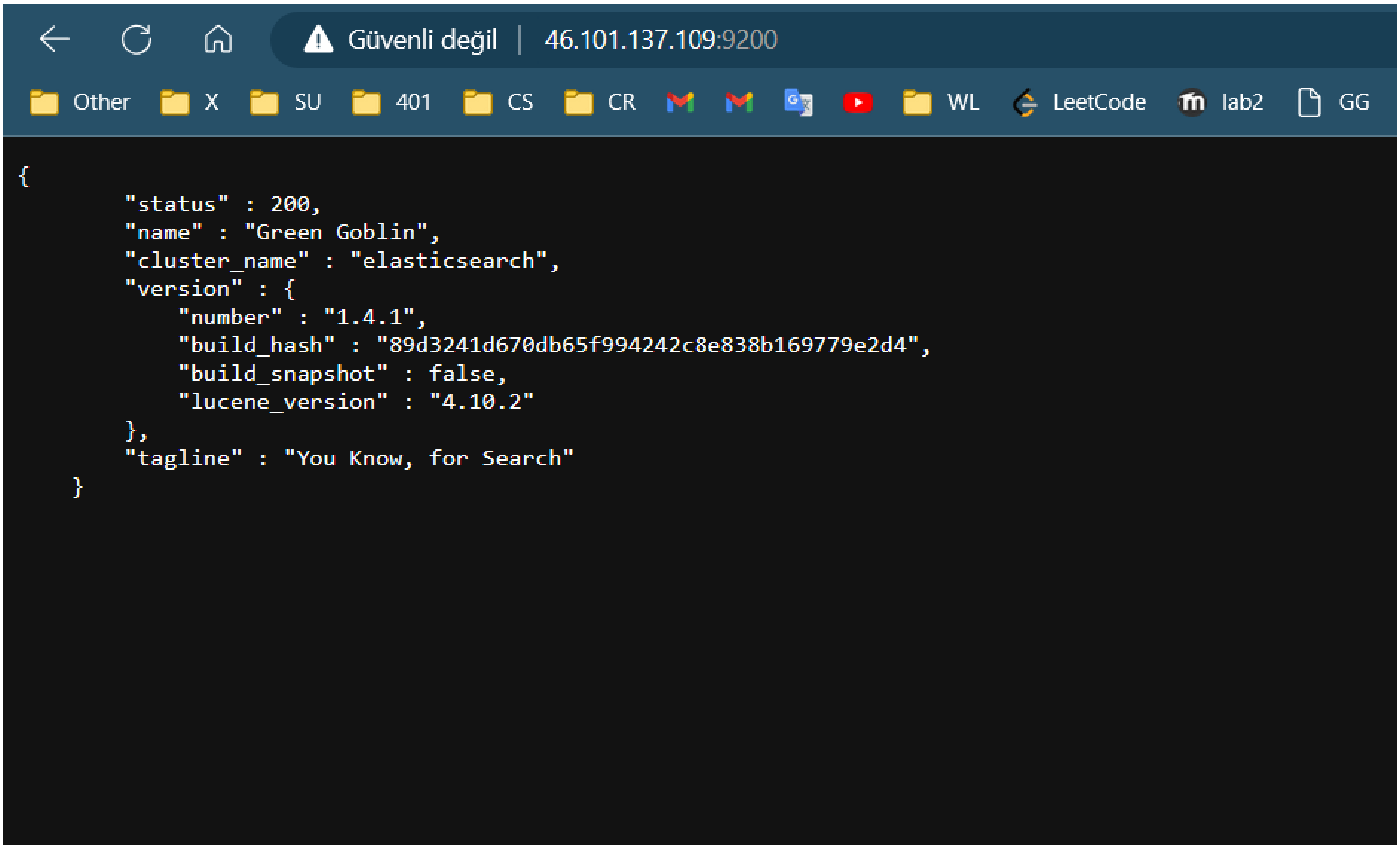
*Figure 1: Installing Elastichoney*

Then I deployed it by executing the elastichoney without any flag in the background. After entering the command, it did not give any output to the terminal to indicate whether it is running or not; therefore, I used 'ss -ltnp' command to see the actively listening TCP ports along with their port numbers and service names. As seen in the screenshot below, elastichoney is currently listening on port 9200. Then I queried it on browser by entering my remote server's public address along with the port number. As seen in screenshot below, the elastichoney service responded with proper elasticsearch 200 code response, and also in the terminal, it logged my request. After I saw that I've successfully installed elastichoney and managed to deploy it, I killed the process as I will further to installing the other honeypot: elasticpot. Here are the screenshots:



```
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# ./elastichoney &
[1] 36215
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# jobs -l
[1]+ 36215 Running                 ./elastichoney &
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# ss -ltnp
State              Recv-Q             Send-Q                         Local Address:Port                          Peer Address:Port             Process
LISTEN             0                  4096                              127.0.0.54:53                                  0.0.0.0:*                 users:(("systemd-resolve",pid=474,fd=16))
LISTEN             0                  4096                           127.0.0.53%lo:53                                  0.0.0.0:*                 users:(("systemd-resolve",pid=474,fd=14))
LISTEN             0                  4096                                       *:9200                                      *:*                 users:(("elastichoney",pid=36215,fd=5))
LISTEN             0                  4096                                       *:22                                        *:*                 users:(("sshd",pid=826,fd=3),("systemd",pid=1,fd=71))
LISTEN             0                  511                                        *:80                                        *:*                 users:(("apache2",pid=9112,fd=4),("apache2",pid=9111,fd=4),("apach
e2",pid=616,fd=4))
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# {
    "source": "159.20.91.222",
    "@timestamp": "2023-11-09T19:02:52.69573475Z",
    "url": "46.101.137.109:9200/",
    "method": "GET",
    "form": "",
    "payload": "",
    "headers": {
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
        "host": "46.101.137.109:9200",
        "content_type": "",
        "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5"
    },
    "type": "recon",
    "honeypot": "46.101.137.109"
}
{
    "source": "159.20.91.222",
    "@timestamp": "2023-11-09T19:02:52.873247277Z",
    "url": "46.101.137.109:9200/favicon.ico",
    "method": "GET",
    "form": "",
    "payload": "",
    "headers": {
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
        "host": "46.101.137.109:9200",
        "content_type": "",
        "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5"
    },
    "type": "recon",
    "honeypot": "46.101.137.109"
}

root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# kill 36215
[1]+  Exit 2                  ./elastichoney
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney#
```

*Figure 2: Testing Deployment*

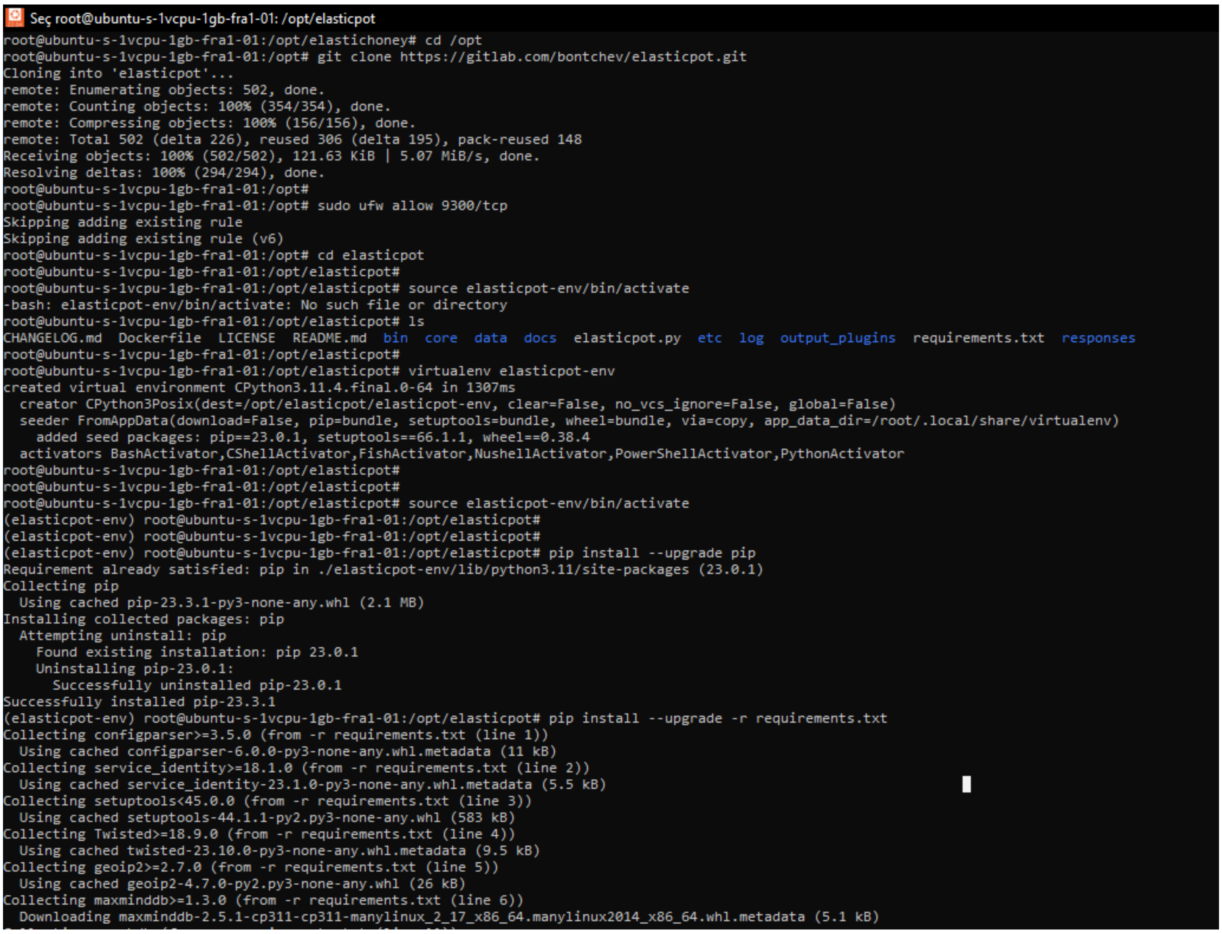


```
{
        "status" : 200,
        "name" : "Green Goblin",
        "cluster_name" : "elasticsearch",
        "version" : {
            "number" : "1.4.1",
            "build_hash" : "89d3241d670db65f994242c8e838b169779e2d4",
            "build_snapshot" : false,
            "lucene_version" : "4.10.2"
        },
        "tagline" : "You Know, for Search"
    }
```

*Figure 3: Response for the query*

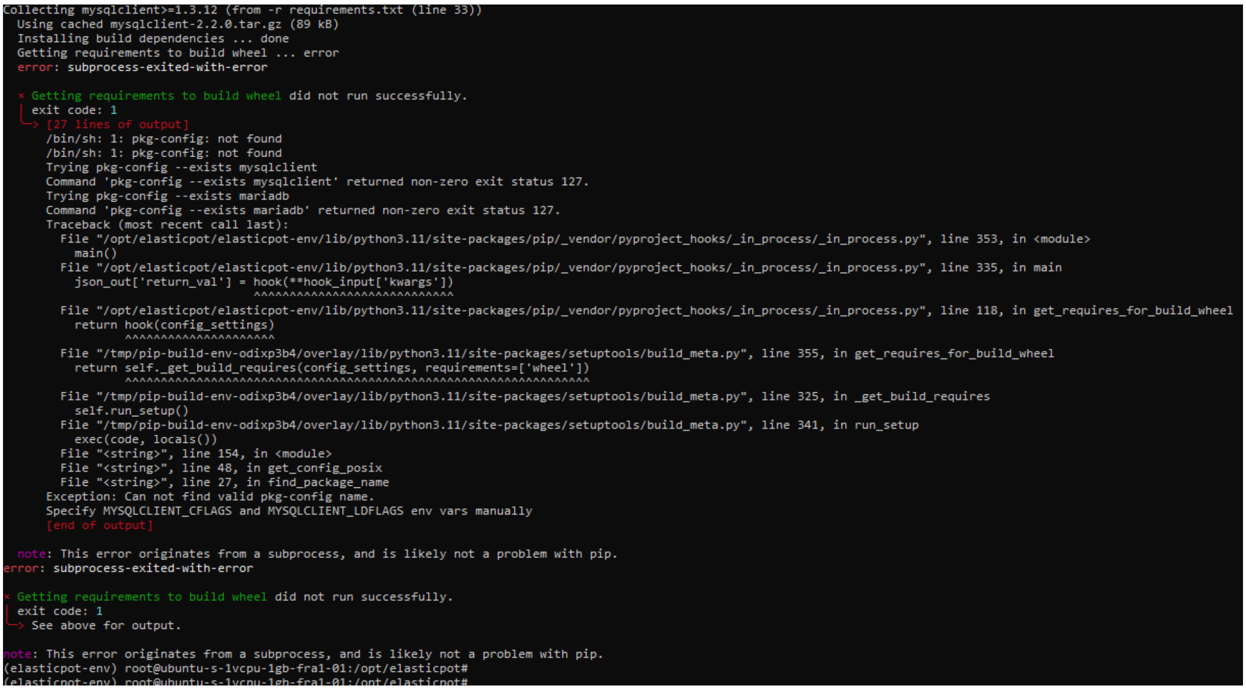
## Installing and deploying *Elasticpot*:

For this honeypot, I've followed the instructions written by the creator of it on github repo. At the very beginning, I've installed the dependencies such as git for cloning the repo, bunch of python packages for the virtual environment etc. Then I cloned the git repo to "/opt", and created the virtual environment as instructed. Then I installed some other python-related packages in the virtual environment. However, installation of some requirements could not be completed, though I didn't quite understand how or why.



```
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elastichoney# cd /opt
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt# git clone https://gitlab.com/bontchev/elasticpot.git
Cloning into 'elasticpot'...
remote: Enumerating objects: 502, done.
remote: Counting objects: 100% (354/354), done.
remote: Compressing objects: 100% (156/156), done.
remote: Total 502 (delta 226), reused 306 (delta 195), pack-reused 148
Receiving objects: 100% (502/502), 121.63 KiB | 5.07 MiB/s, done.
Resolving deltas: 100% (294/294), done.
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt# sudo ufw allow 9300/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt# cd elasticpot
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# source elasticpot-env/bin/activate
-bash: elasticpot-env/bin/activate: No such file or directory
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# ls
CHANGELOG.md  Dockerfile  LICENSE  README.md  bin  core  data  docs  elasticpot.py  etc  log  output_plugins  requirements.txt  responses
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# virtualenv elasticpot-env
created virtual environment CPython3.11.4.final.0-64 in 1307ms
  creator CPython3Posix(dest=/opt/elasticpot/elasticpot-env, clear=False, no_vcs_ignore=False, global=False)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy, app_data_dir=/root/.local/share/virtualenv)
    added seed packages: pip==23.0.1, setuptools==66.1.1, wheel==0.38.4
  activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowerShellActivator,PythonActivator
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# source elasticpot-env/bin/activate
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# pip install --upgrade pip
Requirement already satisfied: pip in ./elasticpot-env/lib/python3.11/site-packages (23.0.1)
Collecting pip
  Using cached pip-23.3.1-py3-none-any.whl (2.1 MB)
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 23.0.1
    Uninstalling pip-23.0.1:
      Successfully uninstalled pip-23.0.1
Successfully installed pip-23.3.1
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# pip install --upgrade -r requirements.txt
Collecting configparser>=3.5.0 (from -r requirements.txt (line 1))
  Using cached configparser-6.0.0-py3-none-any.whl.metadata (11 kB)
Collecting service_identity>=18.1.0 (from -r requirements.txt (line 2))
  Using cached service_identity-23.1.0-py3-none-any.whl.metadata (5.5 kB)
Collecting setuptools<45.0.0 (from -r requirements.txt (line 3))
  Using cached setuptools-44.1.1-py2.py3-none-any.whl (583 kB)
Collecting Twisted>=18.9.0 (from -r requirements.txt (line 4))
  Using cached twisted-23.10.0-py3-none-any.whl.metadata (9.5 kB)
Collecting geoip2>=2.7.0 (from -r requirements.txt (line 5))
  Using cached geoip2-4.7.0-py2.py3-none-any.whl (26 kB)
Collecting maxminddb>=1.3.0 (from -r requirements.txt (line 6))
  Downloading maxminddb-2.5.1-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (5.1 kB)
```

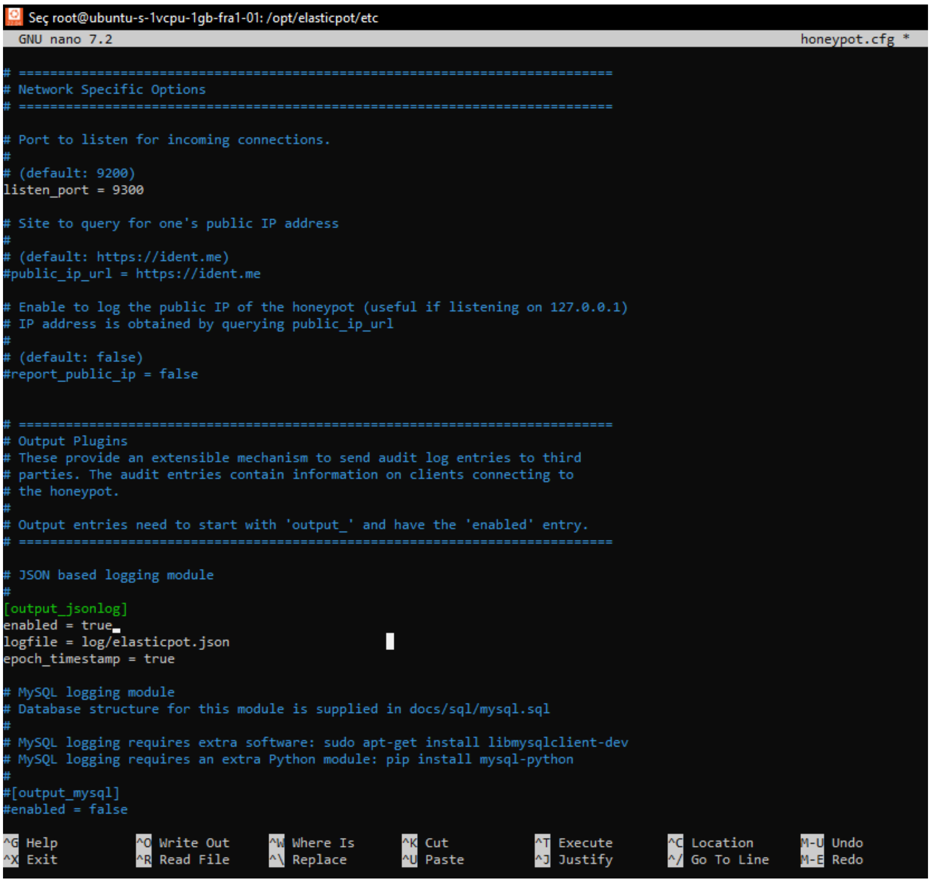
*Figure 4: Installing elasticpot*



```
Collecting mysqlclient>=1.3.12 (from -r requirements.txt (line 33))
  Using cached mysqlclient-2.2.0.tar.gz (89 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... error
  error: subprocess-exited-with-error

  × Getting requirements to build wheel did not run successfully.
  │ exit code: 1
  ╰─> [27 lines of output]
      /bin/sh: 1: pkg-config: not found
      /bin/sh: 1: pkg-config: not found
      Trying pkg-config --exists mysqlclient
      Command 'pkg-config --exists mysqlclient' returned non-zero exit status 127.
      Trying pkg-config --exists mariadb
      Command 'pkg-config --exists mariadb' returned non-zero exit status 127.
      Traceback (most recent call last):
        File "/opt/elasticpot/elasticpot-env/lib/python3.11/site-packages/pip/_vendor/pyproject_hooks/_in_process/_in_process.py", line 353, in <module>
          main()
        File "/opt/elasticpot/elasticpot-env/lib/python3.11/site-packages/pip/_vendor/pyproject_hooks/_in_process/_in_process.py", line 335, in main
          json_out['return_val'] = hook(**hook_input['kwargs'])
                                   ^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        File "/opt/elasticpot/elasticpot-env/lib/python3.11/site-packages/pip/_vendor/pyproject_hooks/_in_process/_in_process.py", line 118, in get_requires_for_build_wheel
          return hook(config_settings)
                 ^^^^^^^^^^^^^^^^^^^^^
        File "/tmp/pip-build-env-odixp3b4/overlay/lib/python3.11/site-packages/setuptools/build_meta.py", line 355, in get_requires_for_build_wheel
          return self._get_build_requires(config_settings, requirements=['wheel'])
                 ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        File "/tmp/pip-build-env-odixp3b4/overlay/lib/python3.11/site-packages/setuptools/build_meta.py", line 325, in _get_build_requires
          self.run_setup()
        File "/tmp/pip-build-env-odixp3b4/overlay/lib/python3.11/site-packages/setuptools/build_meta.py", line 341, in run_setup
          exec(code, locals())
        File "<string>", line 154, in <module>
        File "<string>", line 48, in get_config_posix
        File "<string>", line 27, in find_package_name
      Exception: Can not find valid pkg-config name.
      Specify MYSQLCLIENT_CFLAGS and MYSQLCLIENT_LDFLAGS env vars manually
      [end of output]

  note: This error originates from a subprocess, and is likely not a problem with pip.
error: subprocess-exited-with-error

× Getting requirements to build wheel did not run successfully.
│ exit code: 1
╰─> See above for output.

note: This error originates from a subprocess, and is likely not a problem with pip.
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
```

*Figure 5: Problems during installation of dependencies in requirements.txt*

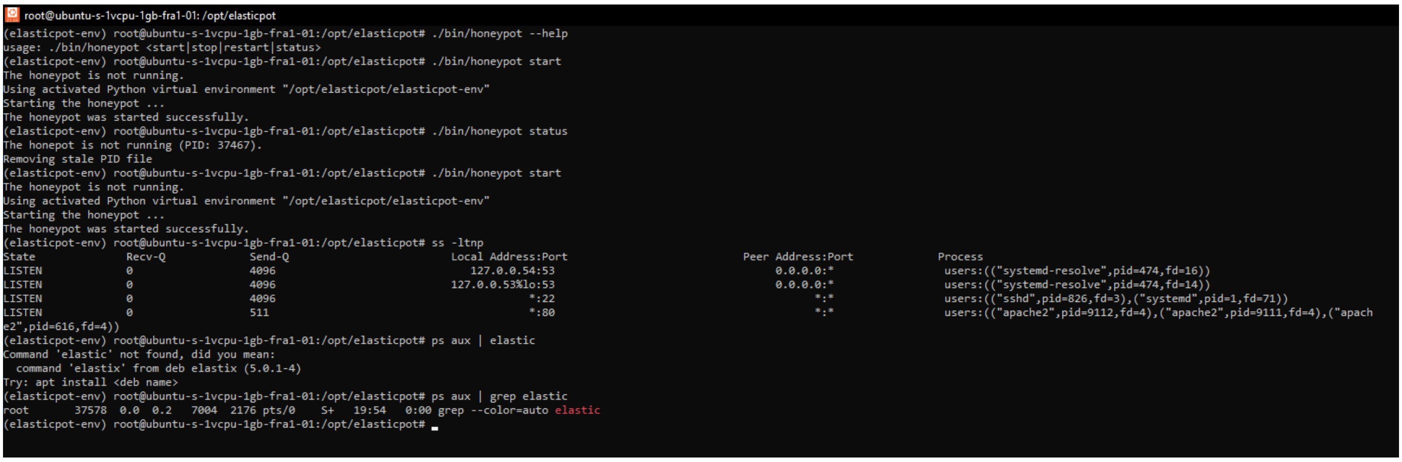
Still, I continued to follow the next steps in instructions. As the creator of the service explains in instructions, if user wants to change some configurations, it is needed to copy ‘honeypot.cfg.base’ file as ‘honeypot.cfg’ and overwrite the copied file, since the program prioritizes .cfg file rather than .cfg.base ones. So, I copied it and opened with nano to make some adjustments. I’ve changed the port number to 9300, and enabled JSON logging which provides more verbose and organised results. I also copied ‘honeypot-launch.cfg.base’ with the name ‘honeypot-launch.cfg’, which will includes configurations about virtual environment. Here are the adjustments on ‘honeypot.cfg’ file:



```
Seç root@ubuntu-s-1vcpu-1gb-fra1-01: /opt/elasticpot/etc
  GNU nano 7.2                                                                    honeypot.cfg *

# ============================================================================
# Network Specific Options
# ============================================================================

# Port to listen for incoming connections.
#
# (default: 9200)
listen_port = 9300

# Site to query for one's public IP address
#
# (default: https://ident.me)
#public_ip_url = https://ident.me

# Enable to log the public IP of the honeypot (useful if listening on 127.0.0.1)
# IP address is obtained by querying public_ip_url
#
# (default: false)
#report_public_ip = false


# ============================================================================
# Output Plugins
# These provide an extensible mechanism to send audit log entries to third
# parties. The audit entries contain information on clients connecting to
# the honeypot.
#
# Output entries need to start with 'output_' and have the 'enabled' entry.
# ============================================================================

# JSON based logging module
#
[output_jsonlog]
enabled = true
logfile = log/elasticpot.json
epoch_timestamp = true

# MySQL logging module
# Database structure for this module is supplied in docs/sql/mysql.sql
#
# MySQL logging requires extra software: sudo apt-get install libmysqlclient-dev
# MySQL logging requires an extra Python module: pip install mysql-python
#
#[output_mysql]
#enabled = false
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo
```

*Figure 6: Customizing configurations of elasticpot*

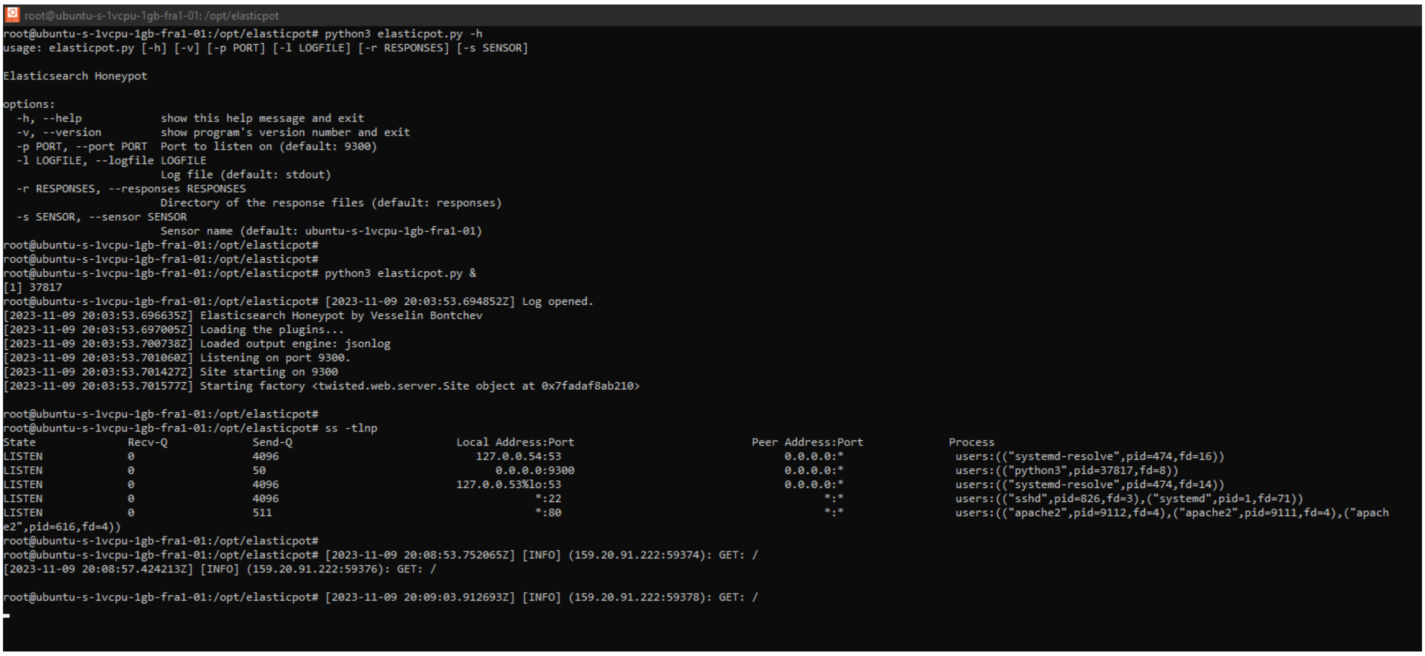
Then I run the executable in bin folder to deploy the honeypot, but even though it says the honeypot is started, it seems it terminates after printing some information. To be sure, I’ve checked the ports and active processes but as seen below, elasticpot it is not running.



```
root@ubuntu-s-1vcpu-1gb-fra1-01: /opt/elasticpot
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# ./bin/honeypot --help
usage: ./bin/honeypot <start|stop|restart|status>
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# ./bin/honeypot start
The honeypot is not running.
Using activated Python virtual environment "/opt/elasticpot/elasticpot-env"
Starting the honeypot ...
The honeypot was started successfully.
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# ./bin/honeypot status
The honepot is not running (PID: 37467).
Removing stale PID file
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# ./bin/honeypot start
The honeypot is not running.
Using activated Python virtual environment "/opt/elasticpot/elasticpot-env"
Starting the honeypot ...
The honeypot was started successfully.
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# ss -ltnp
State          Recv-Q         Send-Q                  Local Address:Port                     Peer Address:Port            Process
LISTEN         0              4096                       127.0.0.54:53                            0.0.0.0:*                users:(("systemd-resolve",pid=474,fd=16))
LISTEN         0              4096                    127.0.0.53%lo:53                            0.0.0.0:*                users:(("systemd-resolve",pid=474,fd=14))
LISTEN         0              4096                             *:22                                  *:*                users:(("sshd",pid=826,fd=3),("systemd",pid=1,fd=71))
LISTEN         0              511                              *:80                                  *:*                users:(("apache2",pid=9112,fd=4),("apache2",pid=9111,fd=4),("apach
e2",pid=616,fd=4))
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# ps aux | elastic
Command 'elastic' not found, did you mean:
  command 'elastix' from deb elastix (5.0.1-4)
Try: apt install <deb name>
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# ps aux | grep elastic
root       37578  0.0  0.2   7004  2176 pts/0    S+   19:54   0:00 grep --color=auto elastic
(elasticpot-env) root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# 
```

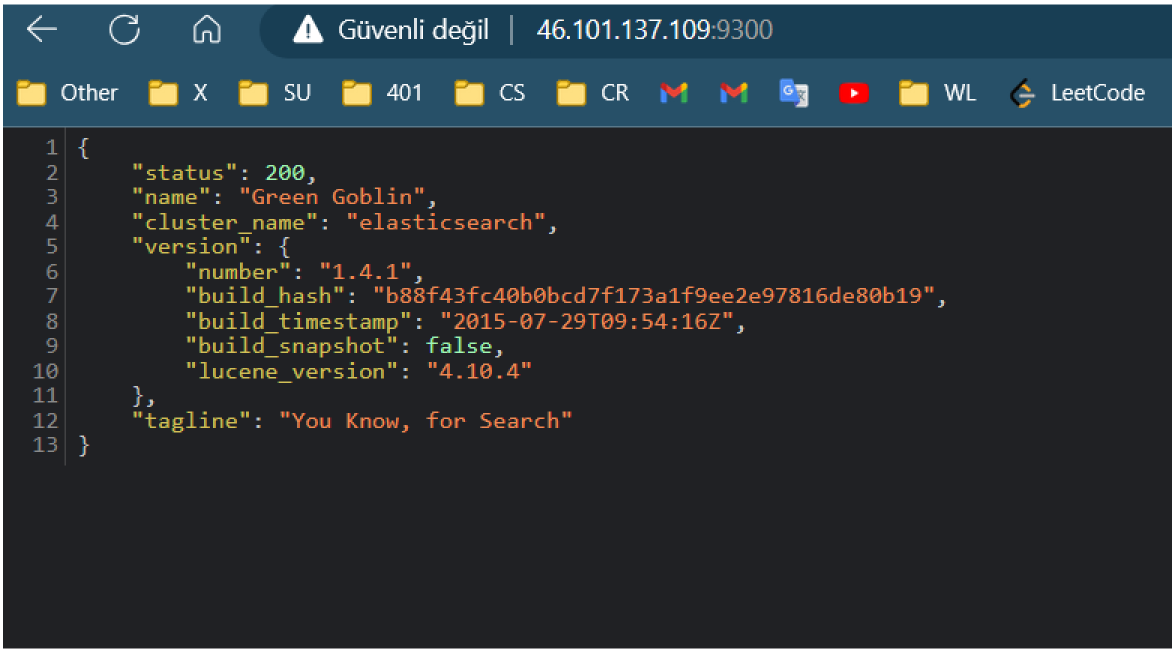
*Figure 7: Trying to deploy elasticpot*

After investigating the situation for long hours, I found out that it stems from the missing dependencies that could not been installed in previous steps. Then I analysed the problem deeper and concluded that the problem is related with the python version. I guess, the executable file in the bin folder was compiled with a different version of python, so something goes wrong while running it. Hopefully, the source code is in the directory, which gave me the idea to manually run the python code with python3. I tried it by entering “python3 elasticpot.py -h” command, and it worked. Then I deployed it and this time it showed a proper log that indicates the service is started. Just to be sure, I again checked the ports and saw that port 9300 is in listening state. Then I sent a query through my browser, and the service responded and the log was shown on terminal, which indicates that the honeypot is deployed successfully.



```
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# python3 elasticpot.py -h
usage: elasticpot.py [-h] [-v] [-p PORT] [-l LOGFILE] [-r RESPONSES] [-s SENSOR]

Elasticsearch Honeypot

options:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit
  -p PORT, --port PORT  Port to listen on (default: 9300)
  -l LOGFILE, --logfile LOGFILE
                        Log file (default: stdout)
  -r RESPONSES, --responses RESPONSES
                        Directory of the response files (default: responses)
  -s SENSOR, --sensor SENSOR
                        Sensor name (default: ubuntu-s-1vcpu-1gb-fra1-01)
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# python3 elasticpot.py &
[1] 37817
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# [2023-11-09 20:03:53.694852Z] Log opened.
[2023-11-09 20:03:53.696635Z] Elasticsearch Honeypot by Vesselin Bontchev
[2023-11-09 20:03:53.697005Z] Loading the plugins...
[2023-11-09 20:03:53.700738Z] Loaded output engine: jsonlog
[2023-11-09 20:03:53.701060Z] Listening on port 9300.
[2023-11-09 20:03:53.701427Z] Site starting on 9300
[2023-11-09 20:03:53.701577Z] Starting factory <twisted.web.server.Site object at 0x7fadaf8ab210>

root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# ss -tlnp
State            Recv-Q           Send-Q                     Local Address:Port                   Peer Address:Port             Process
LISTEN           0                4096                          127.0.0.54:53                          0.0.0.0:*                 users:(("systemd-resolve",pid=474,fd=16))
LISTEN           0                50                               0.0.0.0:9300                        0.0.0.0:*                 users:(("python3",pid=37817,fd=8))
LISTEN           0                4096                       127.0.0.53%lo:53                          0.0.0.0:*                 users:(("systemd-resolve",pid=474,fd=14))
LISTEN           0                4096                                   *:22                                *:*                 users:(("sshd",pid=826,fd=3),("systemd",pid=1,fd=71))
LISTEN           0                511                                    *:80                                *:*                 users:(("apache2",pid=9112,fd=4),("apache2",pid=9111,fd=4),("apach
e2",pid=616,fd=4))
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot#
root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# [2023-11-09 20:08:53.752065Z] [INFO] (159.20.91.222:59374): GET: /
[2023-11-09 20:08:57.424213Z] [INFO] (159.20.91.222:59376): GET: /

root@ubuntu-s-1vcpu-1gb-fra1-01:/opt/elasticpot# [2023-11-09 20:09:03.912693Z] [INFO] (159.20.91.222:59378): GET: /
```

*Figure 8: Testing Deployment*

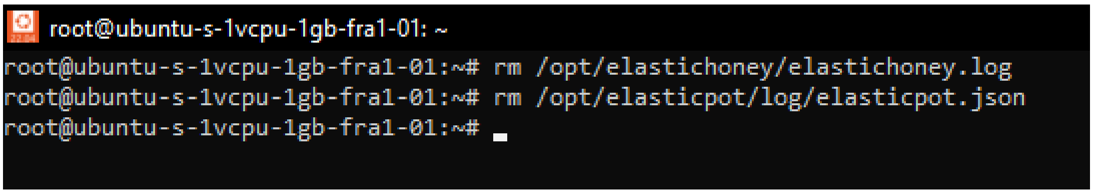


```
{
    "status": 200,
    "name": "Green Goblin",
    "cluster_name": "elasticsearch",
    "version": {
        "number": "1.4.1",
        "build_hash": "b88f43fc40b0bcd7f173a1f9ee2e97816de80b19",
        "build_timestamp": "2015-07-29T09:54:16Z",
        "build_snapshot": false,
        "lucene_version": "4.10.4"
    },
    "tagline": "You Know, for Search"
}
```

*Figure 9: Response for the query*

# Queries:

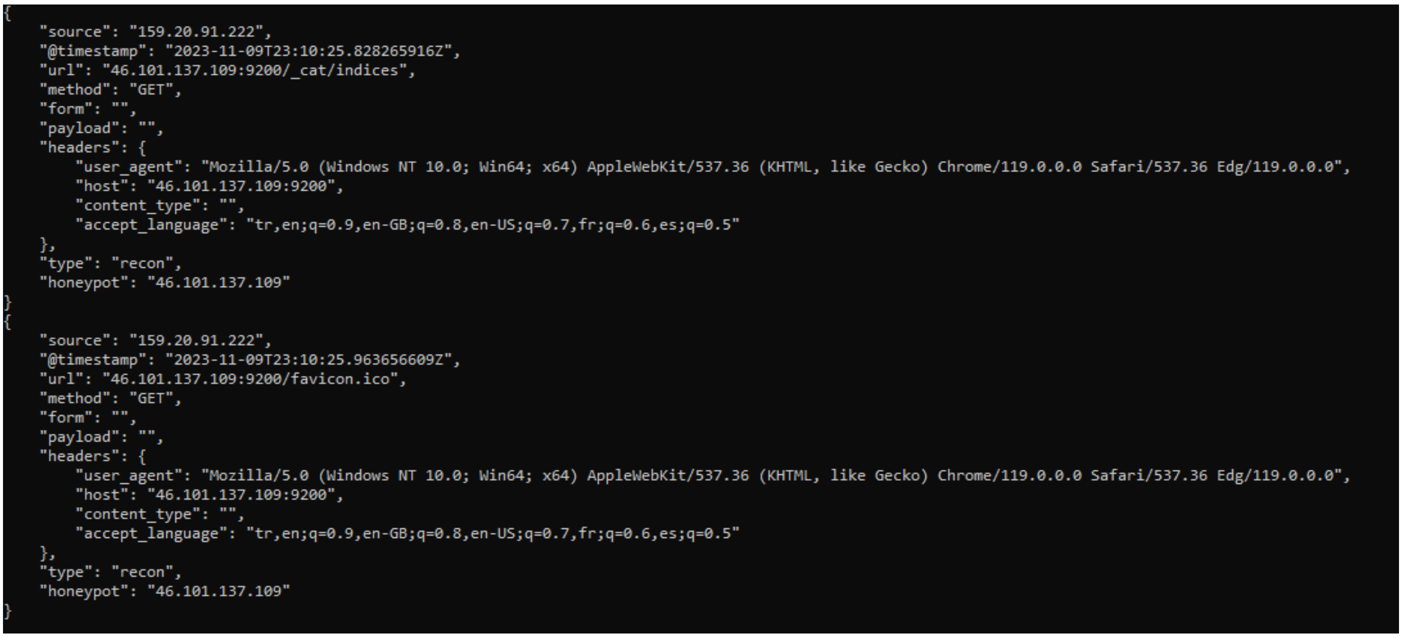
Before starting to perform queries, I've cleaned both honeypots' log files:



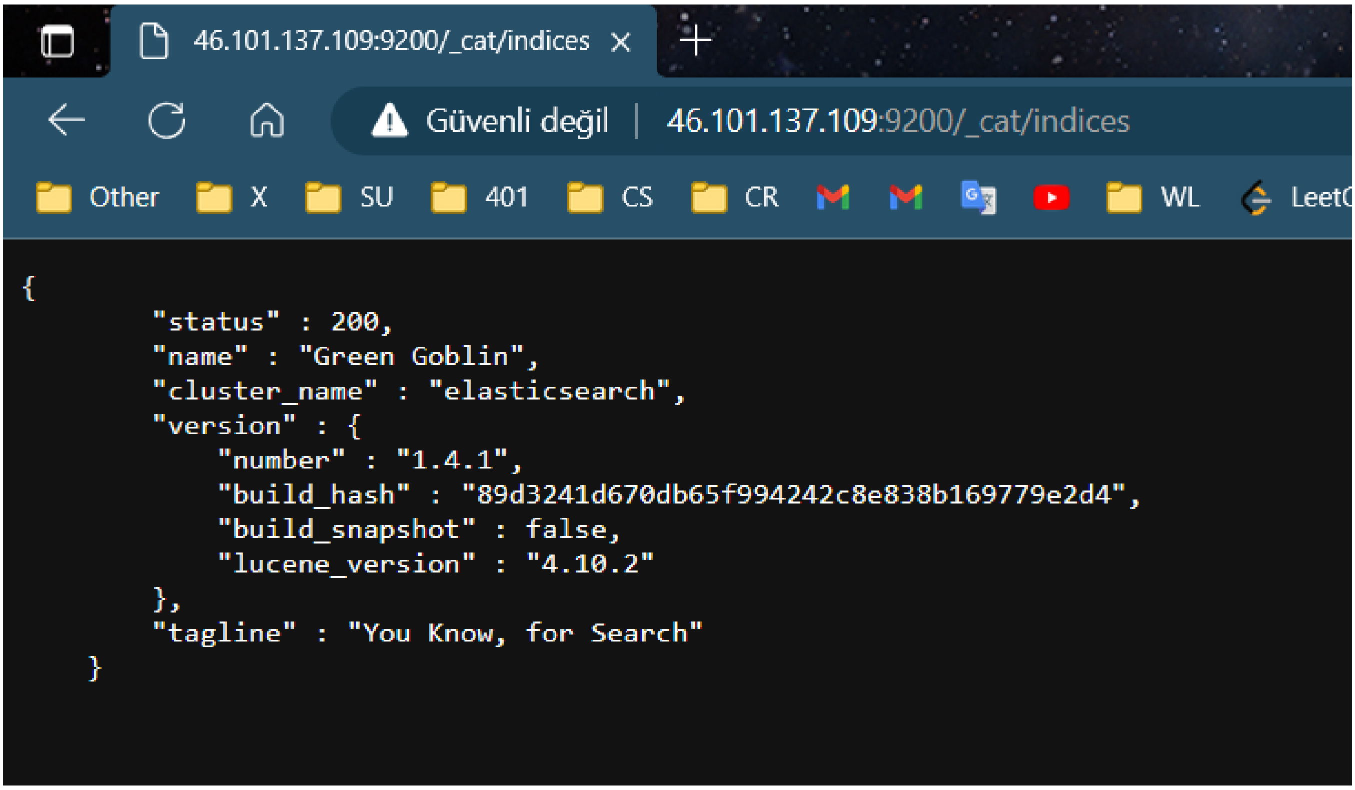
```
root@ubuntu-s-1vcpu-1gb-fra1-01:~# rm /opt/elastichoney/elastichoney.log
root@ubuntu-s-1vcpu-1gb-fra1-01:~# rm /opt/elasticpot/log/elasticpot.json
root@ubuntu-s-1vcpu-1gb-fra1-01:~# _
```

# elastichoney:

## Query 1 = "/_cat/indices" :



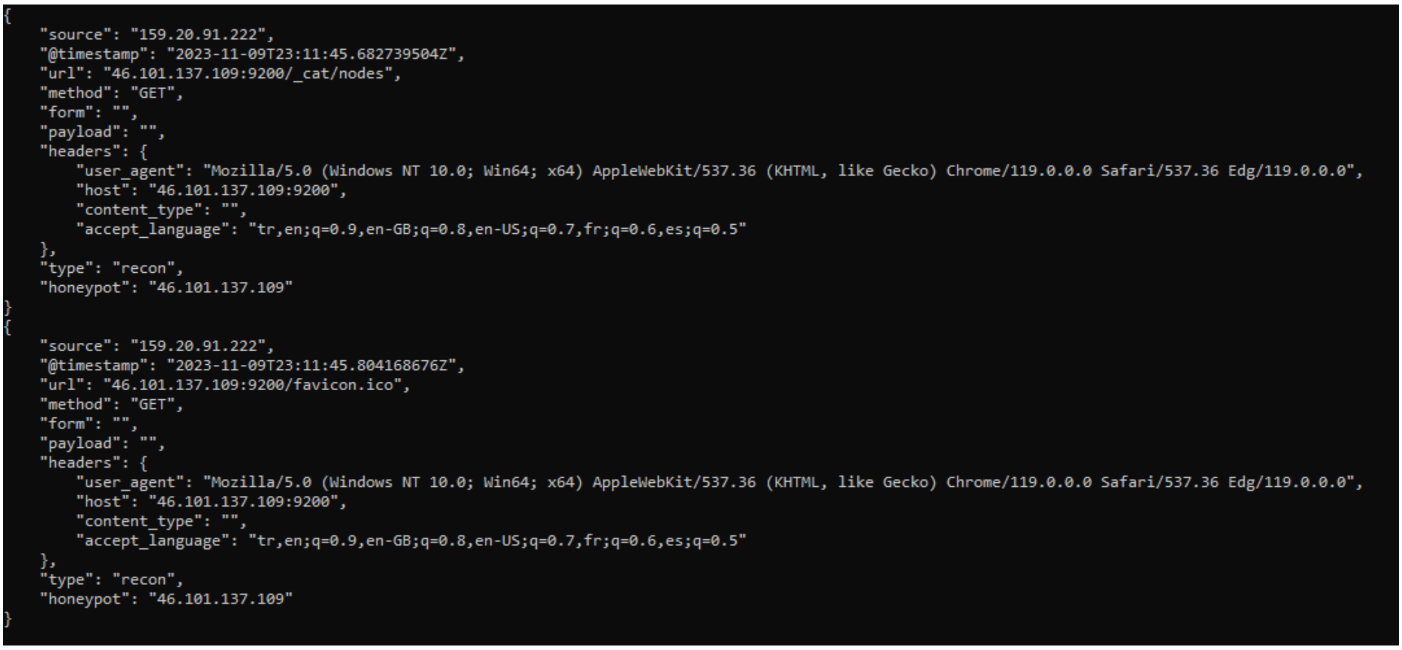
```
{
    "source": "159.20.91.222",
    "@timestamp": "2023-11-09T23:10:25.828265916Z",
    "url": "46.101.137.109:9200/_cat/indices",
    "method": "GET",
    "form": "",
    "payload": "",
    "headers": {
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
        "host": "46.101.137.109:9200",
        "content_type": "",
        "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5"
    },
    "type": "recon",
    "honeypot": "46.101.137.109"
}
{

    "source": "159.20.91.222",
    "@timestamp": "2023-11-09T23:10:25.963656609Z",
    "url": "46.101.137.109:9200/favicon.ico",
    "method": "GET",
    "form": "",
    "payload": "",
    "headers": {
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
        "host": "46.101.137.109:9200",
        "content_type": "",
        "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5"
    },
    "type": "recon",
    "honeypot": "46.101.137.109"
}
```



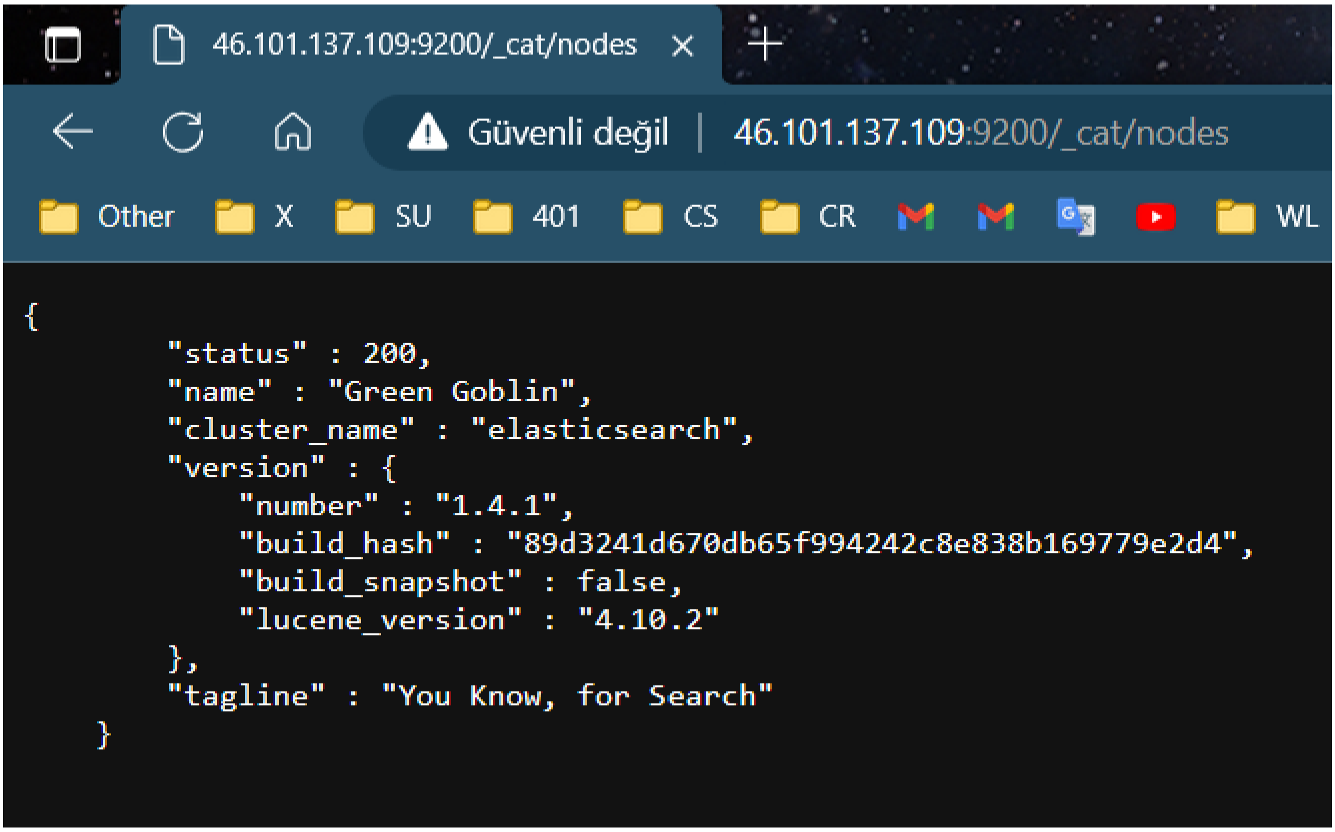
46.101.137.109:9200/_cat/indices
Güvenli değil
46.101.137.109:9200/_cat/indices
Other
X
SU
401
CS
CR
WL
Leet

```
{
        "status" : 200,
        "name" : "Green Goblin",
        "cluster_name" : "elasticsearch",
        "version" : {
            "number" : "1.4.1",
            "build_hash" : "89d3241d670db65f994242c8e838b169779e2d4",
            "build_snapshot" : false,
            "lucene_version" : "4.10.2"
        },
        "tagline" : "You Know, for Search"
    }
```

## Query 2 = “/_cat/nodes” :



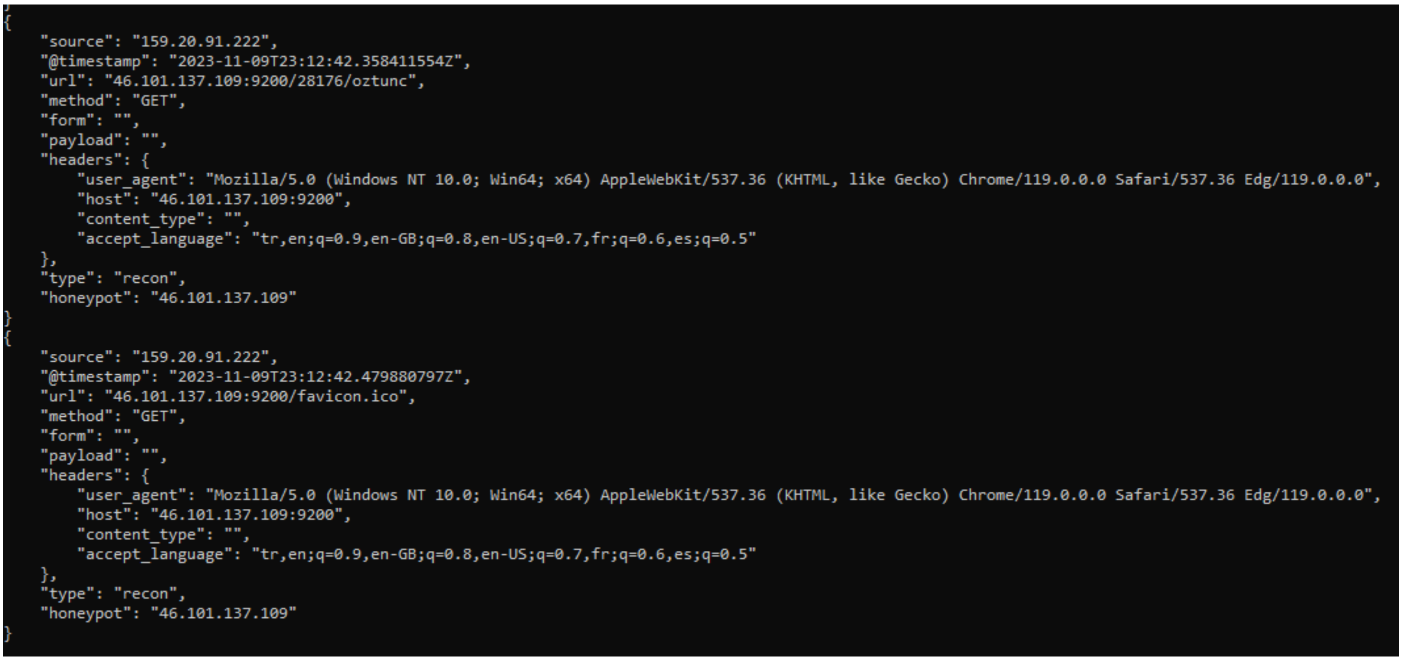
```
{
    "source": "159.20.91.222",
    "@timestamp": "2023-11-09T23:11:45.682739504Z",
    "url": "46.101.137.109:9200/_cat/nodes",
    "method": "GET",
    "form": "",
    "payload": "",
    "headers": {
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
        "host": "46.101.137.109:9200",
        "content_type": "",
        "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5"
    },
    "type": "recon",
    "honeypot": "46.101.137.109"
}
{
    "source": "159.20.91.222",
    "@timestamp": "2023-11-09T23:11:45.804168676Z",
    "url": "46.101.137.109:9200/favicon.ico",
    "method": "GET",
    "form": "",
    "payload": "",
    "headers": {
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
        "host": "46.101.137.109:9200",
        "content_type": "",
        "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5"
    },
    "type": "recon",
    "honeypot": "46.101.137.109"
}
```



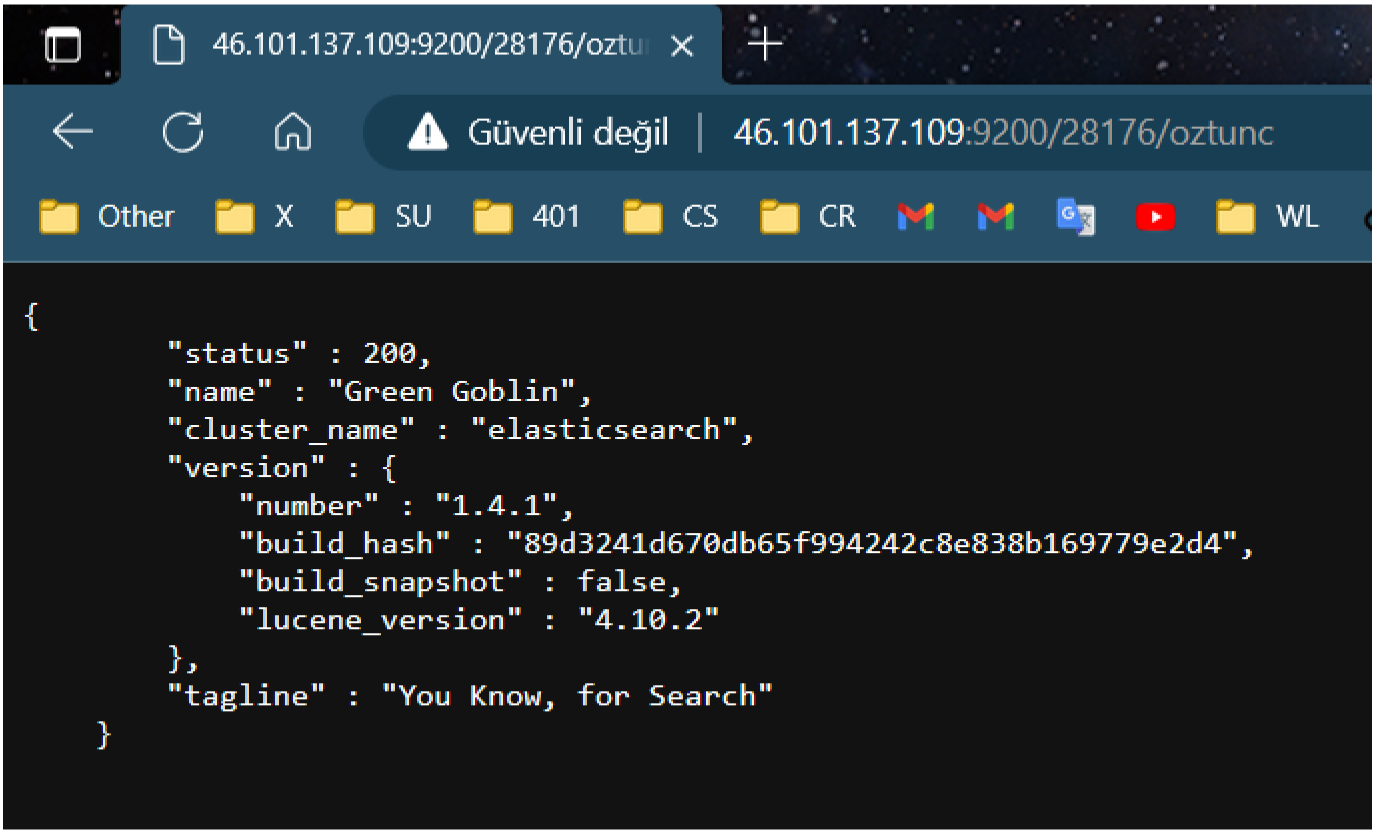
46.101.137.109:9200/_cat/nodes
Güvenli değil
46.101.137.109:9200/_cat/nodes
Other
X
SU
401
CS
CR
WL

```
{
        "status" : 200,
        "name" : "Green Goblin",
        "cluster_name" : "elasticsearch",
        "version" : {
            "number" : "1.4.1",
            "build_hash" : "89d3241d670db65f994242c8e838b169779e2d4",
            "build_snapshot" : false,
            "lucene_version" : "4.10.2"
        },
        "tagline" : "You Know, for Search"
    }
```

**Query  3 = “/28176/oztunc” :**



```
}
{
    "source": "159.20.91.222",
    "@timestamp": "2023-11-09T23:12:42.358411554Z",
    "url": "46.101.137.109:9200/28176/oztunc",
    "method": "GET",
    "form": "",
    "payload": "",
    "headers": {
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
        "host": "46.101.137.109:9200",
        "content_type": "",
        "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5"
    },
    "type": "recon",
    "honeypot": "46.101.137.109"
}
{
    "source": "159.20.91.222",
    "@timestamp": "2023-11-09T23:12:42.479880797Z",
    "url": "46.101.137.109:9200/favicon.ico",
    "method": "GET",
    "form": "",
    "payload": "",
    "headers": {
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
        "host": "46.101.137.109:9200",
        "content_type": "",
        "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5"
    },
    "type": "recon",
    "honeypot": "46.101.137.109"
}
```



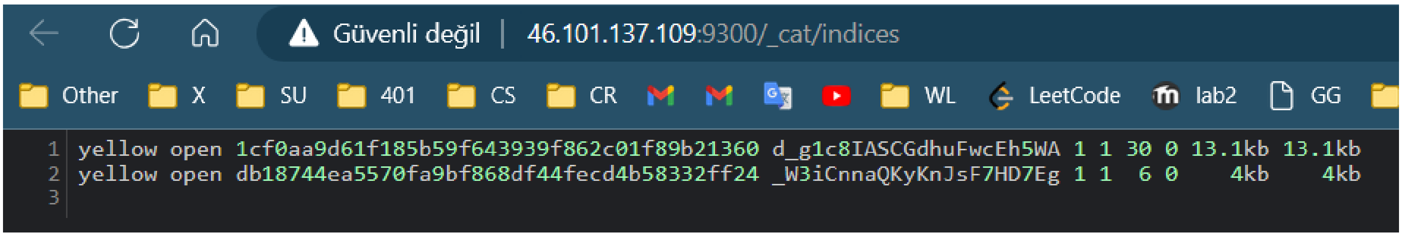
46.101.137.109:9200/28176/oztu
Güvenli değil
46.101.137.109:9200/28176/oztunc
Other
X
SU
401
CS
CR
WL

```
{
        "status" : 200,
        "name" : "Green Goblin",
        "cluster_name" : "elasticsearch",
        "version" : {
            "number" : "1.4.1",
            "build_hash" : "89d3241d670db65f994242c8e838b169779e2d4",
            "build_snapshot" : false,
            "lucene_version" : "4.10.2"
        },
        "tagline" : "You Know, for Search"
    }
```

# elasticpot:

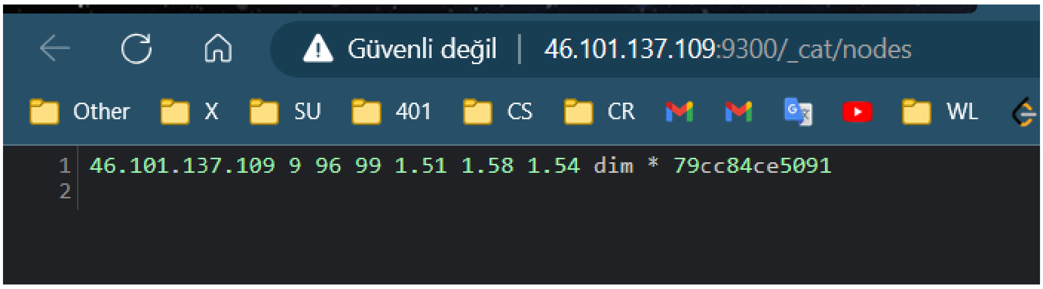
As elasticpot logs one line of limited information to the terminal for each query, I added http responses and added a single terminal screenshot at the end. In addition, there is also the screenshot of the 'elasticpot.json' log file which includes more detailed information in json format. However, for each query log, elasticpot puts the output in a single line which is not readable for a json file. Therefore, I've transferred the file to my local computer via scp and formatted it via VScode for make it more readable. I did not added the screenshot for the log file of elastichoney because it is same as the terminal logs that I added as screenshots.

## Query 1 = "/_cat/indices" :



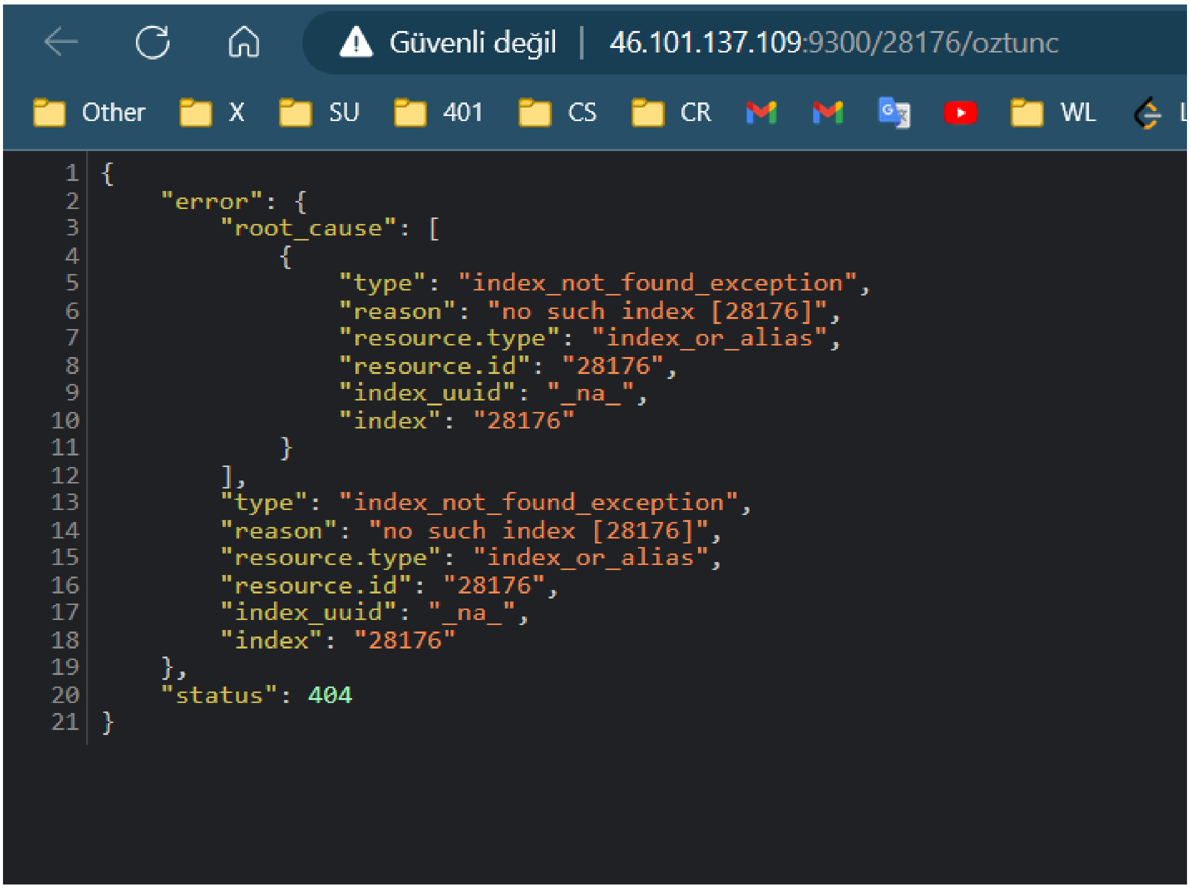
```
yellow open 1cf0aa9d61f185b59f643939f862c01f89b21360 d_g1c8IASCGdhuFwcEh5WA 1 1 30 0 13.1kb 13.1kb
yellow open db18744ea5570fa9bf868df44fecd4b58332ff24 _W3iCnnaQKyKnJsF7HD7Eg 1 1  6 0    4kb    4kb
```

## Query 2 = "/_cat/nodes" :



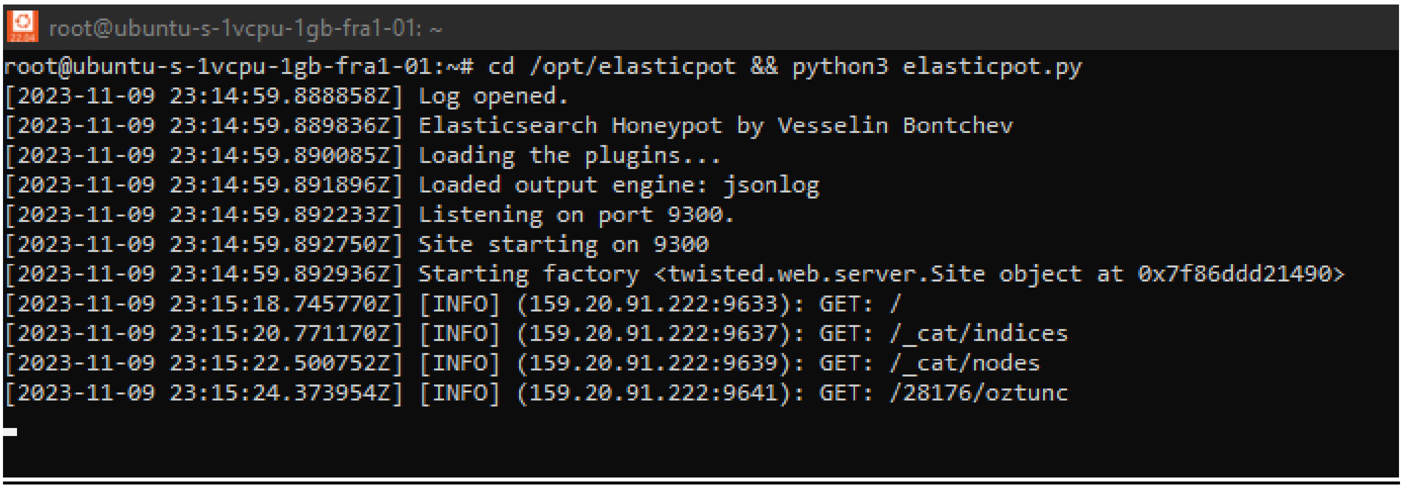
```
46.101.137.109 9 96 99 1.51 1.58 1.54 dim * 79cc84ce5091
```

## Query 3 = "/28176/oztunc" :



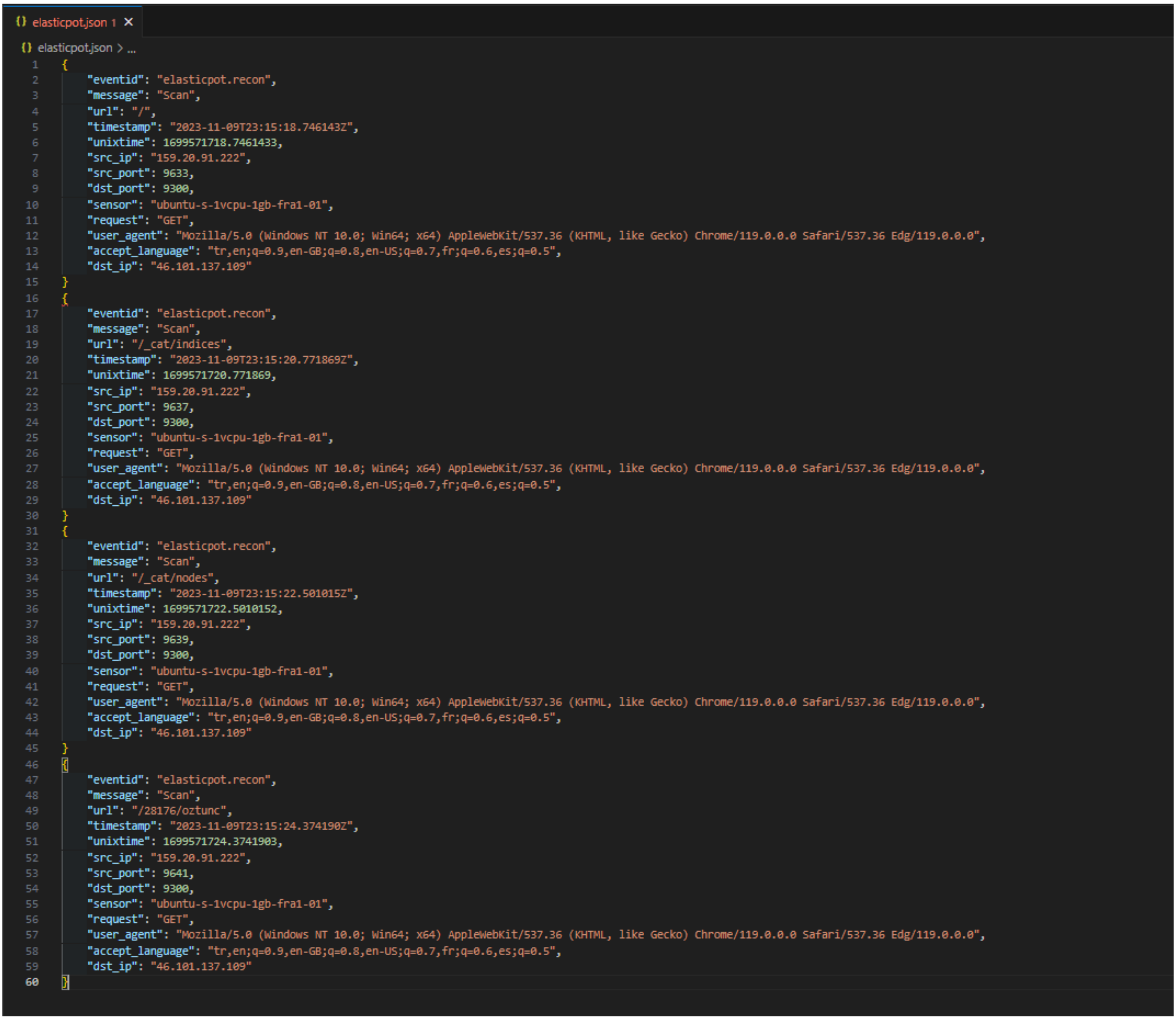
```
{
    "error": {
        "root_cause": [
            {
                "type": "index_not_found_exception",
                "reason": "no such index [28176]",
                "resource.type": "index_or_alias",
                "resource.id": "28176",
                "index_uuid": "_na_",
                "index": "28176"
            }
        ],
        "type": "index_not_found_exception",
        "reason": "no such index [28176]",
        "resource.type": "index_or_alias",
        "resource.id": "28176",
        "index_uuid": "_na_",
        "index": "28176"
    },
    "status": 404
}
```

## Terminal logs:



```
root@ubuntu-s-1vcpu-1gb-fra1-01:~# cd /opt/elasticpot && python3 elasticpot.py
[2023-11-09 23:14:59.888858Z] Log opened.
[2023-11-09 23:14:59.889836Z] Elasticsearch Honeypot by Vesselin Bontchev
[2023-11-09 23:14:59.890085Z] Loading the plugins...
[2023-11-09 23:14:59.891896Z] Loaded output engine: jsonlog
[2023-11-09 23:14:59.892233Z] Listening on port 9300.
[2023-11-09 23:14:59.892750Z] Site starting on 9300
[2023-11-09 23:14:59.892936Z] Starting factory <twisted.web.server.Site object at 0x7f86ddd21490>
[2023-11-09 23:15:18.745770Z] [INFO] (159.20.91.222:9633): GET: /
[2023-11-09 23:15:20.771170Z] [INFO] (159.20.91.222:9637): GET: /_cat/indices
[2023-11-09 23:15:22.500752Z] [INFO] (159.20.91.222:9639): GET: /_cat/nodes
[2023-11-09 23:15:24.373954Z] [INFO] (159.20.91.222:9641): GET: /28176/oztunc
```

## JSON logs:



```
{
    "eventid": "elasticpot.recon",
    "message": "Scan",
    "url": "/",
    "timestamp": "2023-11-09T23:15:18.746143Z",
    "unixtime": 1699571718.7461433,
    "src_ip": "159.20.91.222",
    "src_port": 9633,
    "dst_port": 9300,
    "sensor": "ubuntu-s-1vcpu-1gb-fra1-01",
    "request": "GET",
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
    "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5",
    "dst_ip": "46.101.137.109"
}
{
    "eventid": "elasticpot.recon",
    "message": "Scan",
    "url": "/_cat/indices",
    "timestamp": "2023-11-09T23:15:20.771869Z",
    "unixtime": 1699571720.771869,
    "src_ip": "159.20.91.222",
    "src_port": 9637,
    "dst_port": 9300,
    "sensor": "ubuntu-s-1vcpu-1gb-fra1-01",
    "request": "GET",
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
    "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5",
    "dst_ip": "46.101.137.109"
}
{
    "eventid": "elasticpot.recon",
    "message": "Scan",
    "url": "/_cat/nodes",
    "timestamp": "2023-11-09T23:15:22.501015Z",
    "unixtime": 1699571722.5010152,
    "src_ip": "159.20.91.222",
    "src_port": 9639,
    "dst_port": 9300,
    "sensor": "ubuntu-s-1vcpu-1gb-fra1-01",
    "request": "GET",
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
    "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5",
    "dst_ip": "46.101.137.109"
}
{
    "eventid": "elasticpot.recon",
    "message": "Scan",
    "url": "/28176/oztunc",
    "timestamp": "2023-11-09T23:15:24.374190Z",
    "unixtime": 1699571724.3741903,
    "src_ip": "159.20.91.222",
    "src_port": 9641,
    "dst_port": 9300,
    "sensor": "ubuntu-s-1vcpu-1gb-fra1-01",
    "request": "GET",
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0",
    "accept_language": "tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7,fr;q=0.6,es;q=0.5",
    "dst_ip": "46.101.137.109"
}
```

## Analysis

In my analysis of the two honeypots, Elastichoney and Elasticpot, I find that Elasticpot provides a more comprehensive and realistic emulation of an Elasticsearch server compared to Elastichoney. Elastichoney, as the creator acknowledges in the GitHub repository, is designed to be a simple honeypot project. However, this simplicity might be a limitation in capturing a wide range of attacks effectively. When considering the log files generated by both honeypots, Elasticpot's logs appear to be more informative and detailed. The log entries include valuable information such as the event ID, message, timestamp, source IP, source port, destination port, sensor information, request details, user-agent, and destination IP. In contrast, Elastichoney's logs provide essential details but lack some of the additional information that could be valuable for a more detailed analysis of attacks. In terms of HTTP responses, Elastichoney's approach of using a single hardcoded response for all queries could potentially make it easier for an attacker to distinguish it from a real Elasticsearch server. Elasticpot, on the other hand, employs a variety of responses, enhancing its ability to mimic the behavior of a real server, which eventually makes it more attractive and deceptive for the attackers. If I were to choose a honeypot for capturing attacks towards Elasticsearch servers, I would choose Elasticpot due to its more sophisticated response mechanisms and detailed logging capabilities. The variety of responses and the inclusion of additional information in the logs provide a more realistic environment for simulating potential attacks. Also, the large variety of configuration options of elasticpot when compared to elastichoney, makes elasticpot far more flexible and usable. As for the possible improvements, Elastichoney must have a larger response pool and more configuration options. For elasticpot, the only thing that I can complain and wish to be enhanced is its more complex installation process when compared to elastichoney.

**Remote Server Public IPv4:** 46.101.137.109

**My Local Machine Public IPv4:** 159.20.91.222