Kailash Parshad – Honey-Pots-Logs-To-Elastic-Search-ELK

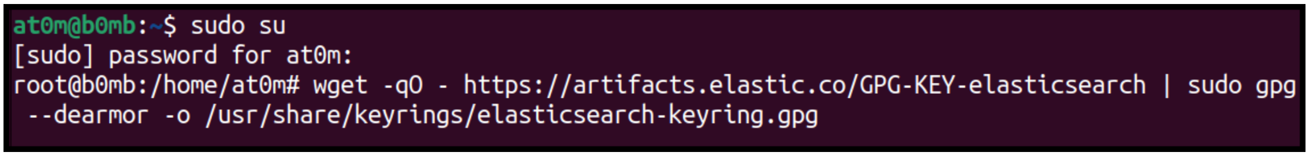
Link: -

https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.html

Download and install the public signing key:

Command: -

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo
gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
```

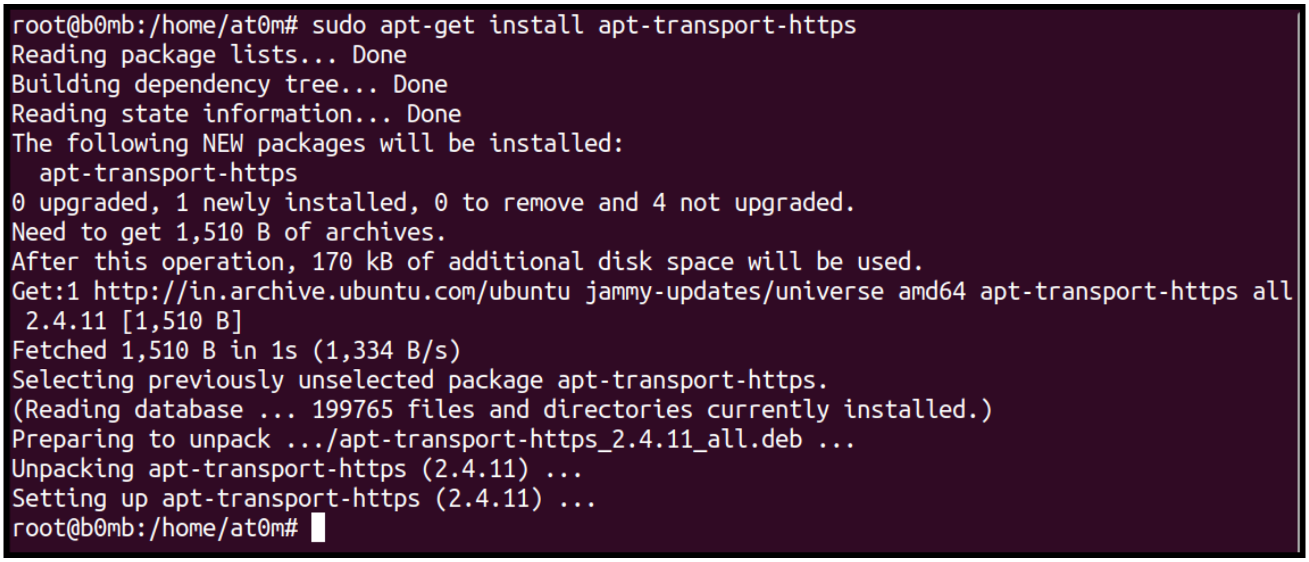


```
at0m@b0mb:~$ sudo su
[sudo] password for at0m:
root@b0mb:/home/at0m# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg
 --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
```

Installing from the APT repository

Command: -

```
sudo apt-get install apt-transport-https
```

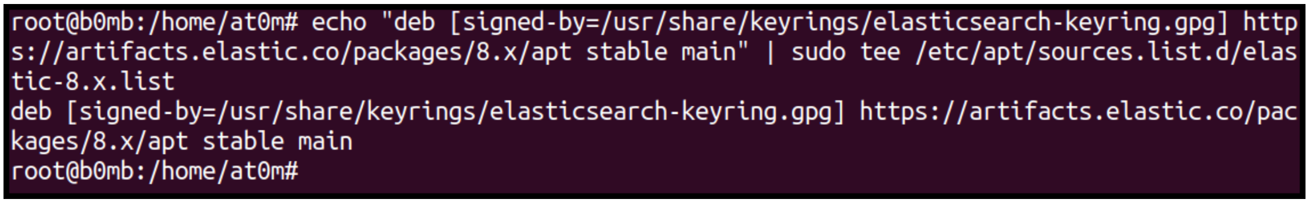


```
root@b0mb:/home/at0m# sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.
Need to get 1,510 B of archives.
After this operation, 170 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 apt-transport-https all
 2.4.11 [1,510 B]
Fetched 1,510 B in 1s (1,334 B/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 199765 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.4.11_all.deb ...
Unpacking apt-transport-https (2.4.11) ...
Setting up apt-transport-https (2.4.11) ...
root@b0mb:/home/at0m# 
```

Save the repository definition to /etc/apt/sources.list.d/elastic-8.x.list

Command: -

```
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg]
https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo
tee /etc/apt/sources.list.d/elastic-8.x.list
```

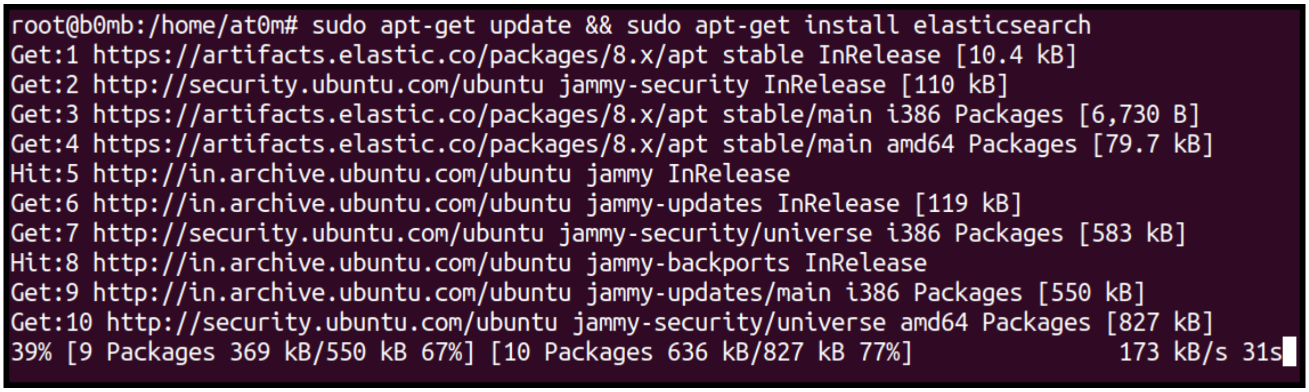


```
root@b0mb:/home/at0m# echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] http
s://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elas
tic-8.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/pac
kages/8.x/apt stable main
root@b0mb:/home/at0m#
```

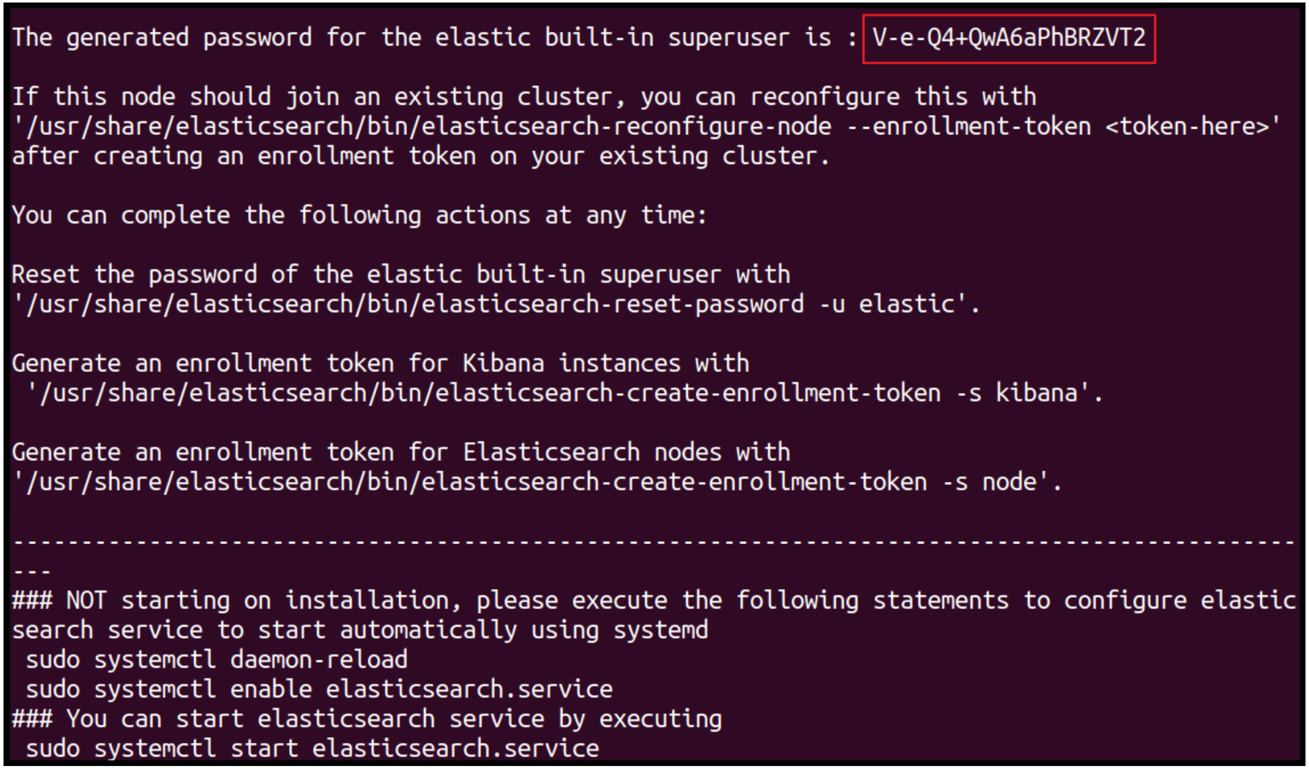
Elasticsearch Debian package install

Command: -

```
sudo apt-get update && sudo apt-get install elasticsearch
```



```
root@b0mb:/home/at0m# sudo apt-get update && sudo apt-get install elasticsearch
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [10.4 kB]
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 https://artifacts.elastic.co/packages/8.x/apt stable/main i386 Packages [6,730 B]
Get:4 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [79.7 kB]
Hit:5 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:6 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [583 kB]
Hit:8 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:9 http://in.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [550 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [827 kB]
39% [9 Packages 369 kB/550 kB 67%] [10 Packages 636 kB/827 kB 77%]               173 kB/s 31s
```

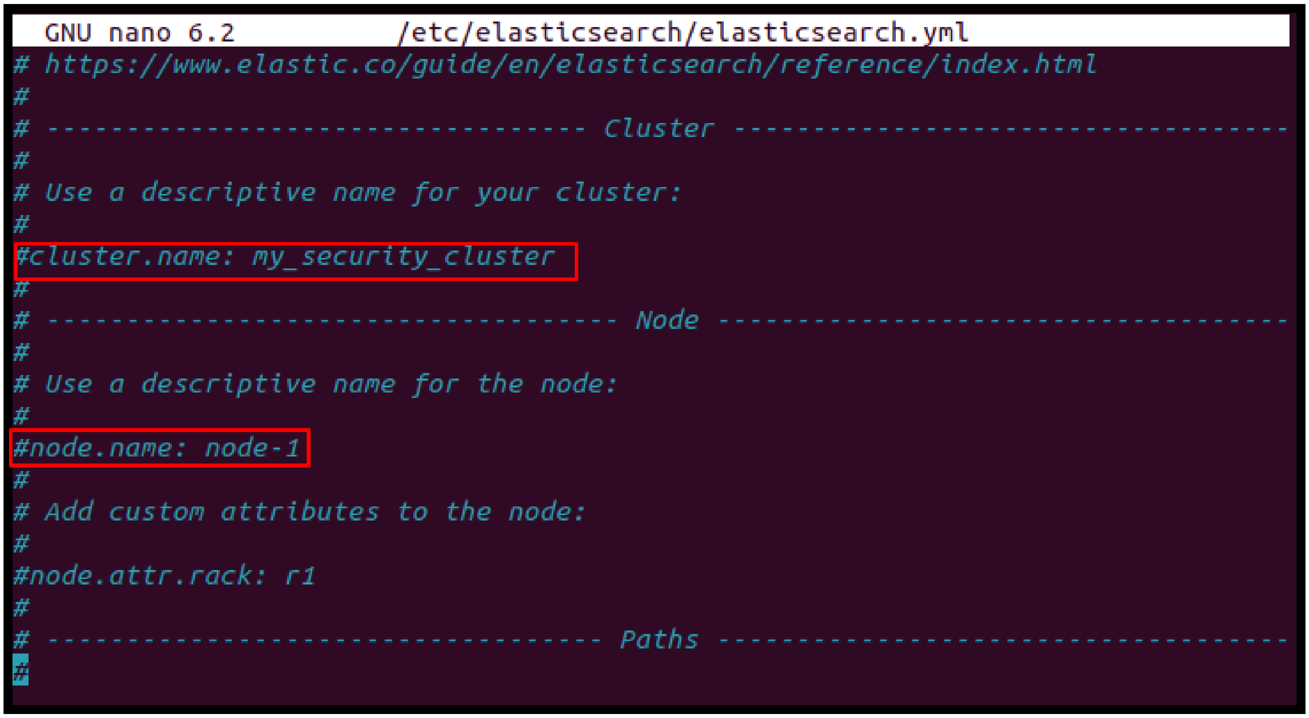


```
The generated password for the elastic built-in superuser is : V-e-Q4+QwA6aPhBRZVT2

If this node should join an existing cluster, you can reconfigure this with
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'
after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:

Reset the password of the elastic built-in superuser with
'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.

Generate an enrollment token for Kibana instances with
 '/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana'.

Generate an enrollment token for Elasticsearch nodes with
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.

----------------------------------------------------------------------------------------------
---
### NOT starting on installation, please execute the following statements to configure elastic
search service to start automatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
```

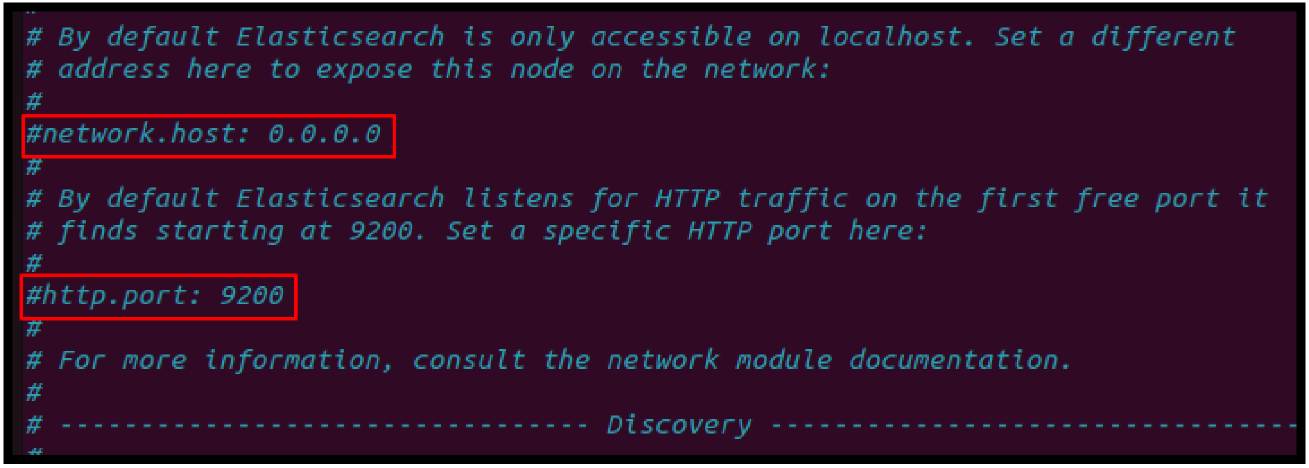
Editing elasticsearch.yml file

Command: -

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```



```
  GNU nano 6.2            /etc/elasticsearch/elasticsearch.yml
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
#cluster.name: my_security_cluster
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
#node.name: node-1
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#
# ----------------------------------- Paths ------------------------------------
#
```



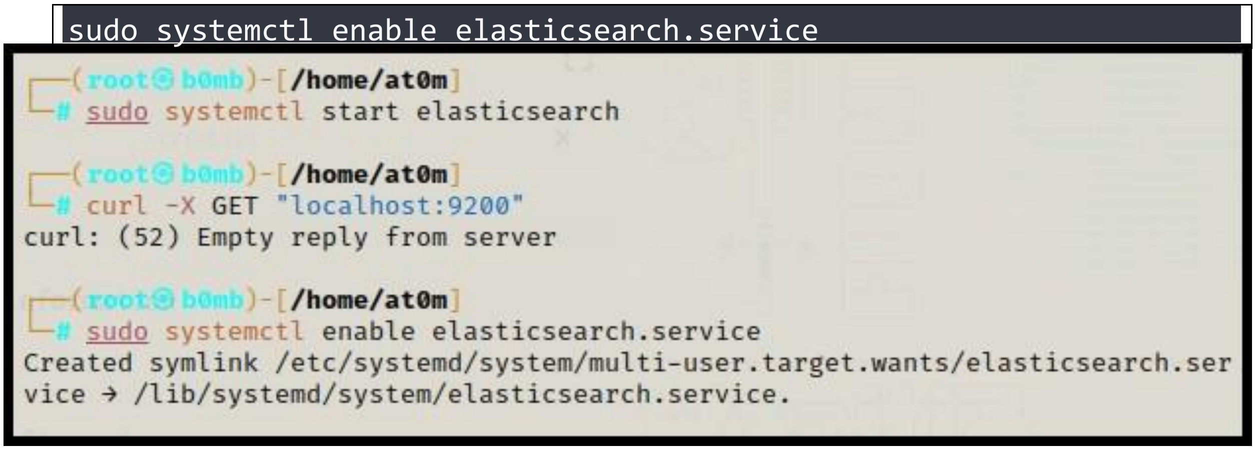
```
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ---------------------------------
```

Starting and Enabling Elastic Search Service

Command: -

```
sudo systemctl start elasticsearch
```

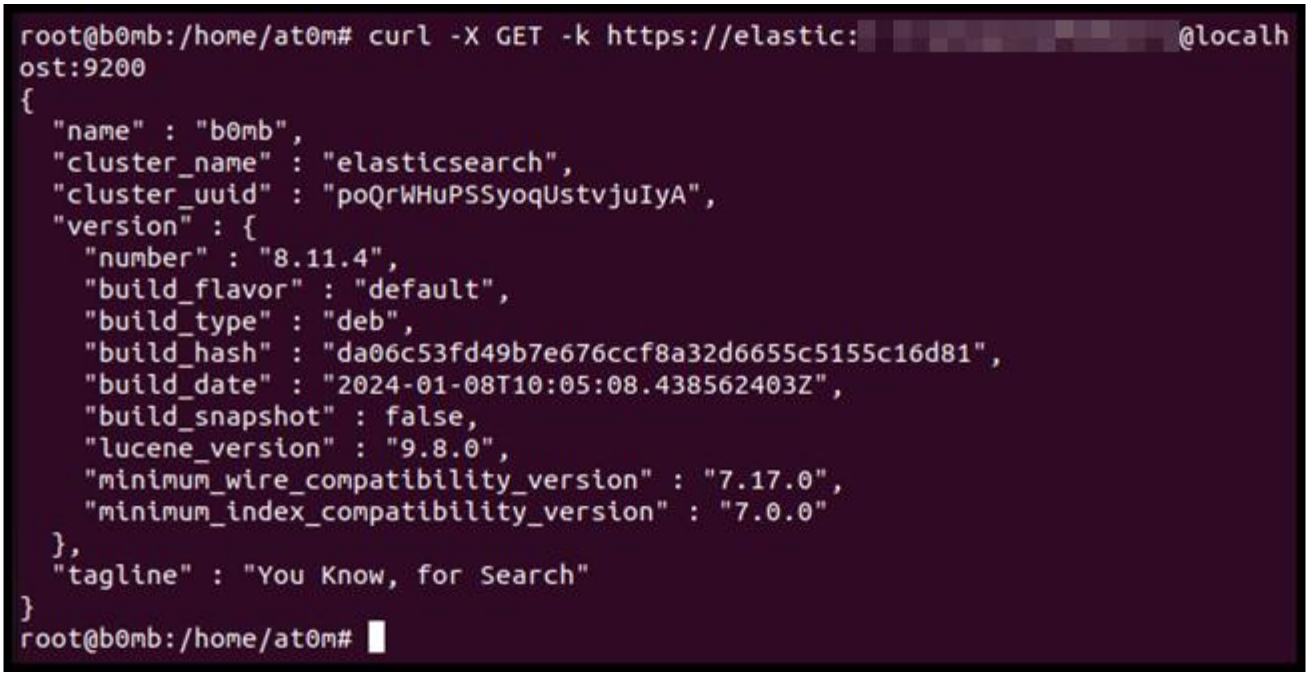
```
sudo systemctl enable elasticsearch.service
```



```
┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl start elasticsearch

┌──(root㉿b0mb)-[/home/at0m]
└─# curl -X GET "localhost:9200"
curl: (52) Empty reply from server

┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.ser
vice → /lib/systemd/system/elasticsearch.service.
```

Starting and Enabling Elastic Search Service

Command: -

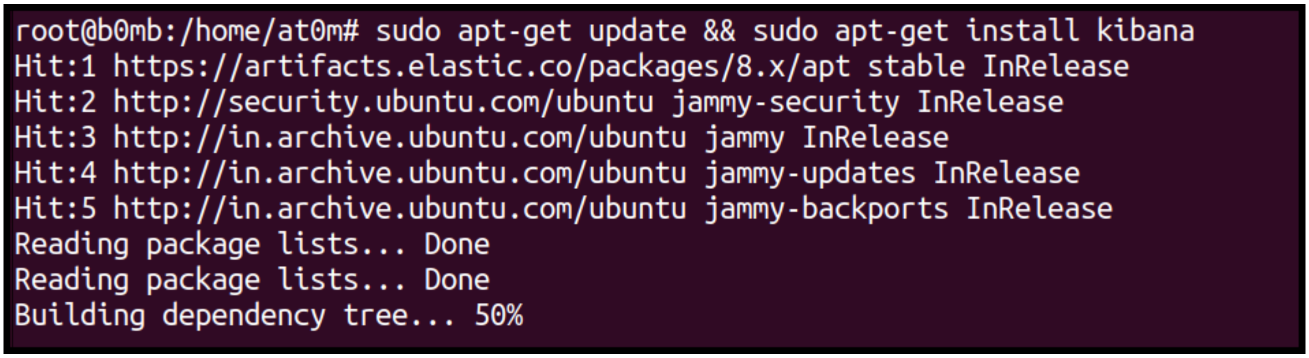


```
root@b0mb:/home/at0m# curl -X GET -k https://elastic:[redacted]@localh
ost:9200
{
  "name" : "b0mb",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "poQrWHuPSSyoqUstvjuIyA",
  "version" : {
    "number" : "8.11.4",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "da06c53fd49b7e676ccf8a32d6655c5155c16d81",
    "build_date" : "2024-01-08T10:05:08.438562403Z",
    "build_snapshot" : false,
    "lucene_version" : "9.8.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
root@b0mb:/home/at0m# 
```

Installing Kibana: -

Command: -

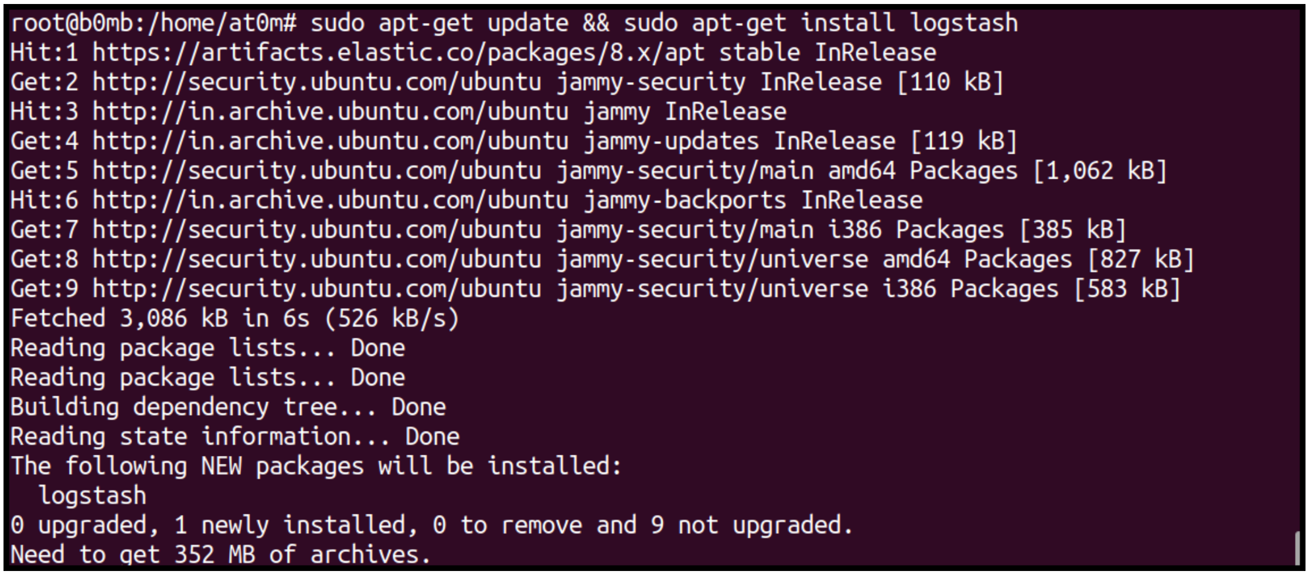
```
sudo apt-get update && sudo apt-get install kibana
```



```
root@b0mb:/home/at0m# sudo apt-get update && sudo apt-get install kibana
Hit:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:5 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... 50%
```

Installing LogStash Command: -

```
sudo apt-get update && sudo apt-get install logstash
```

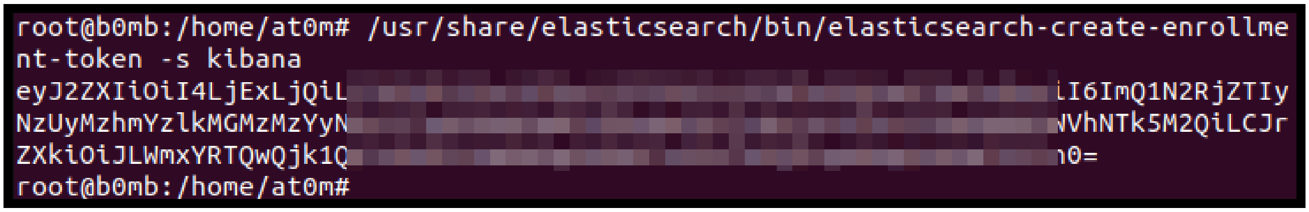


```
root@b0mb:/home/at0m# sudo apt-get update && sudo apt-get install logstash
Hit:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1,062 kB]
Hit:6 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [385 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [827 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [583 kB]
Fetched 3,086 kB in 6s (526 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 9 not upgraded.
Need to get 352 MB of archives.
```

Creating Enrolment Tickets from Elastic for Kibana: -

Command: -

```
/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token
-s kibana
```



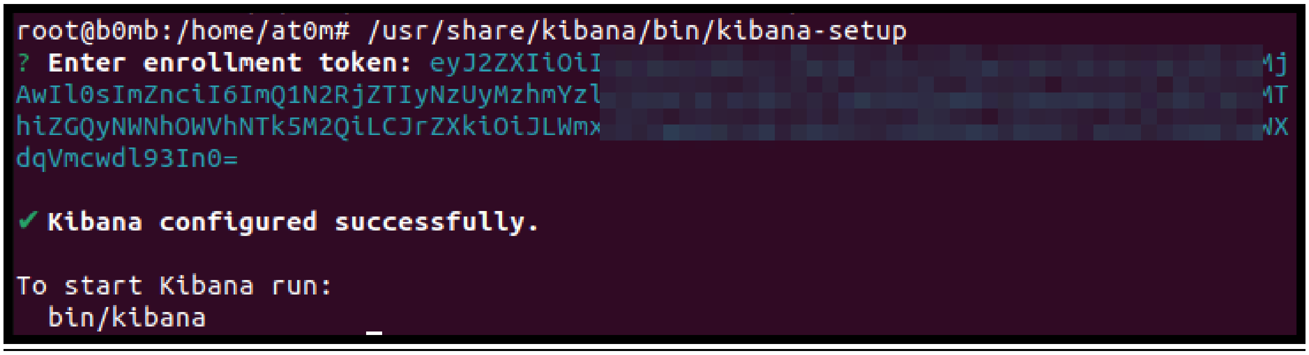
```
root@b0mb:/home/at0m# /usr/share/elasticsearch/bin/elasticsearch-create-enrollme
nt-token -s kibana
eyJ2ZXIiOiI4LjExLjQiL[redacted]iI6ImQ1N2RjZTIy
NzUyMzhmYzlkMGMzMzYyN[redacted]VhNTk5M2QiLCJr
ZXkiOiJLWmxYRTQwQjk1Q[redacted]0=
root@b0mb:/home/at0m#
```

Doing setup of Kibana from the previously generated Enrolment Ticket: -

Command: -

```
/usr/share/kibana/bin/kibana-setup
```

```
<After this Enter the Previous Generated Ticket in the previous
command>
```



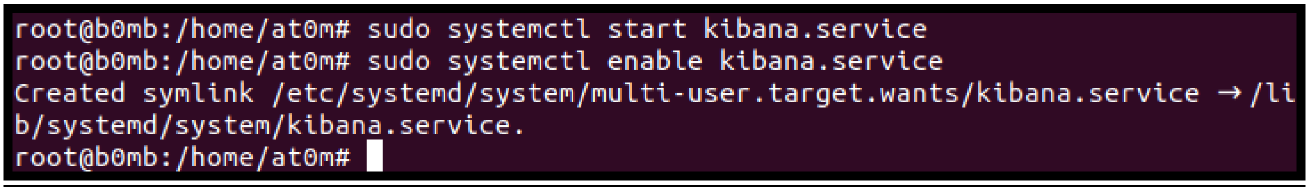
```
root@b0mb:/home/at0m# /usr/share/kibana/bin/kibana-setup
? Enter enrollment token: eyJ2ZXIiOiI[redacted]Mj
AwIl0sImZnciI6ImQ1N2RjZTIyNzUyMzhmYzl                                       MT
hiZGQyNWNhOWVhNTk5M2QiLCJrZXkiOiJLWmx                                       WX
dqVmcwdl93In0=

✓ Kibana configured successfully.

To start Kibana run:
  bin/kibana
```

Starting and Enabling Kibana Service

Command: -

```
sudo systemctl start kibana.service
```

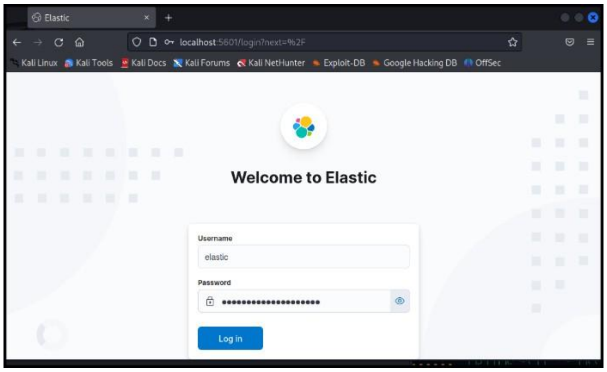
```
sudo systemctl enable kibana.service
```

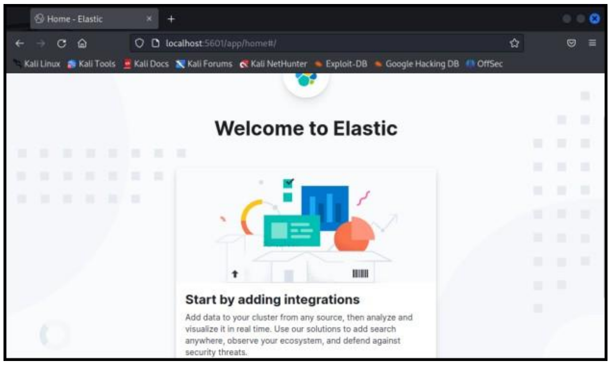


```
root@b0mb:/home/at0m# sudo systemctl start kibana.service
root@b0mb:/home/at0m# sudo systemctl enable kibana.service
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /li
b/systemd/system/kibana.service.
root@b0mb:/home/at0m# 
```

Checking if we can Access Kibana on: -

http://localhost:5601




Home - Elastic
localhost:5601/app/home#/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Welcome to Elastic
Start by adding integrations
Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.

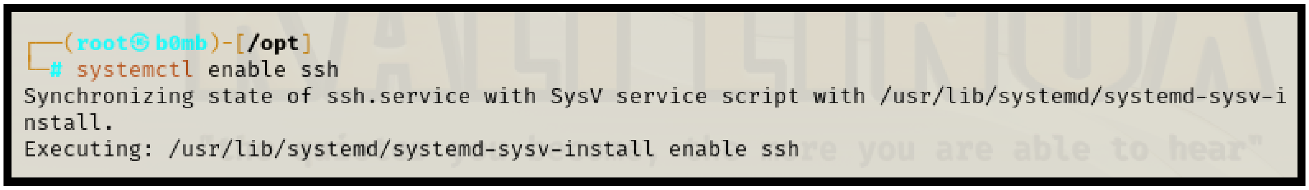
Changing the SSH Port (Target Honeypot Machine): -

```
vi /etc/ssh/sshd_config
```

Download Kippo Honeypot: -

Starting the SSH Service: -

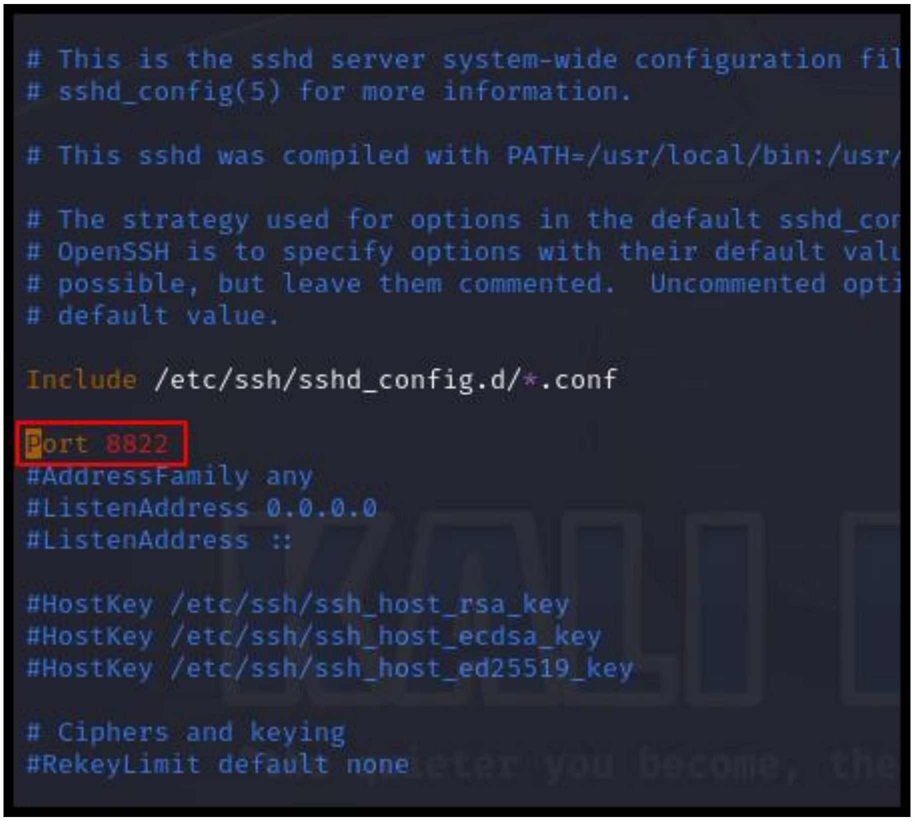
```
systemctl enable ssh
```



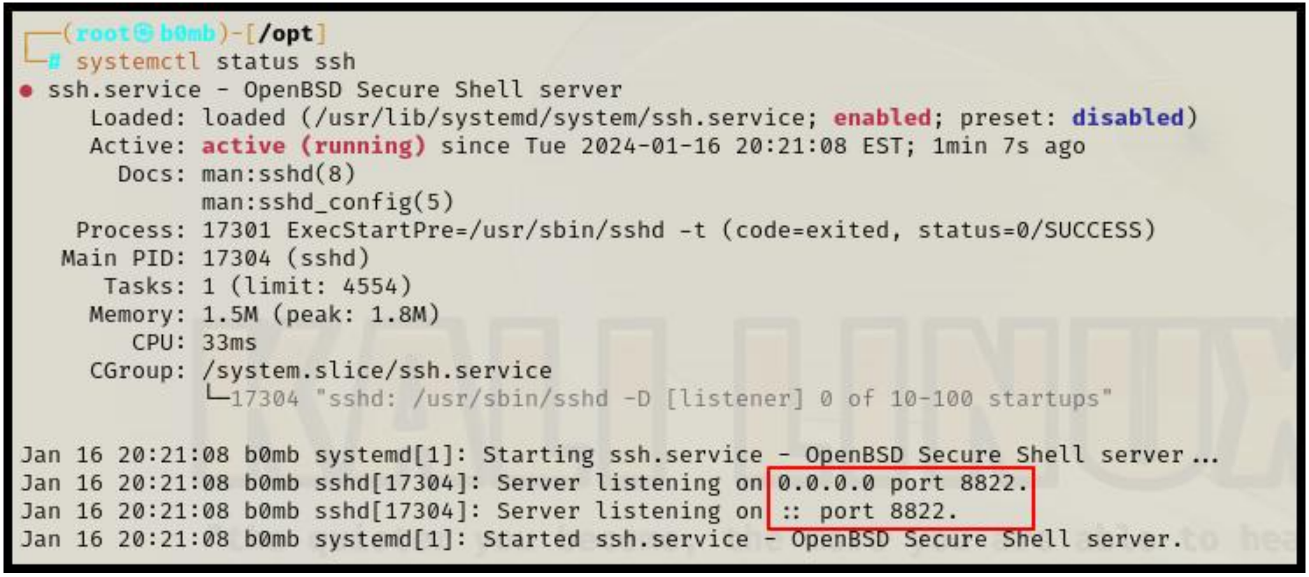
```
┌──(root㉿b0mb)-[/opt]
└─# systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-i
nstall.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
```

Changing the SSH Port:

```
vi /etc/ssh/sshd_config
```



```
# This is the sshd server system-wide configuration fil
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/

# The strategy used for options in the default sshd_cor
# OpenSSH is to specify options with their default valu
# possible, but leave them commented.  Uncommented opti
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 8822
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
```

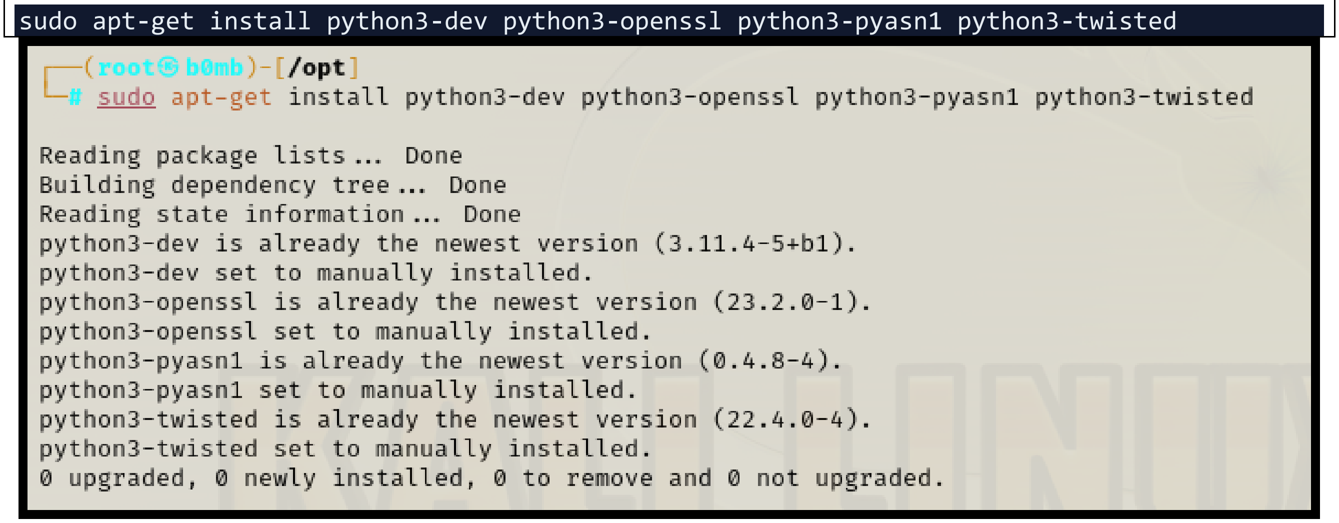


```
┌──(root㉿b0mb)-[/opt]
└─# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
     Active: active (running) since Tue 2024-01-16 20:21:08 EST; 1min 7s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 17301 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 17304 (sshd)
      Tasks: 1 (limit: 4554)
     Memory: 1.5M (peak: 1.8M)
        CPU: 33ms
     CGroup: /system.slice/ssh.service
             └─17304 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 16 20:21:08 b0mb systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 16 20:21:08 b0mb sshd[17304]: Server listening on 0.0.0.0 port 8822.
Jan 16 20:21:08 b0mb sshd[17304]: Server listening on :: port 8822.
Jan 16 20:21:08 b0mb systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

Installing Dependencies

Command: -

```
sudo apt-get install python3-dev python3-openssl python3-pyasn1 python3-twisted
```

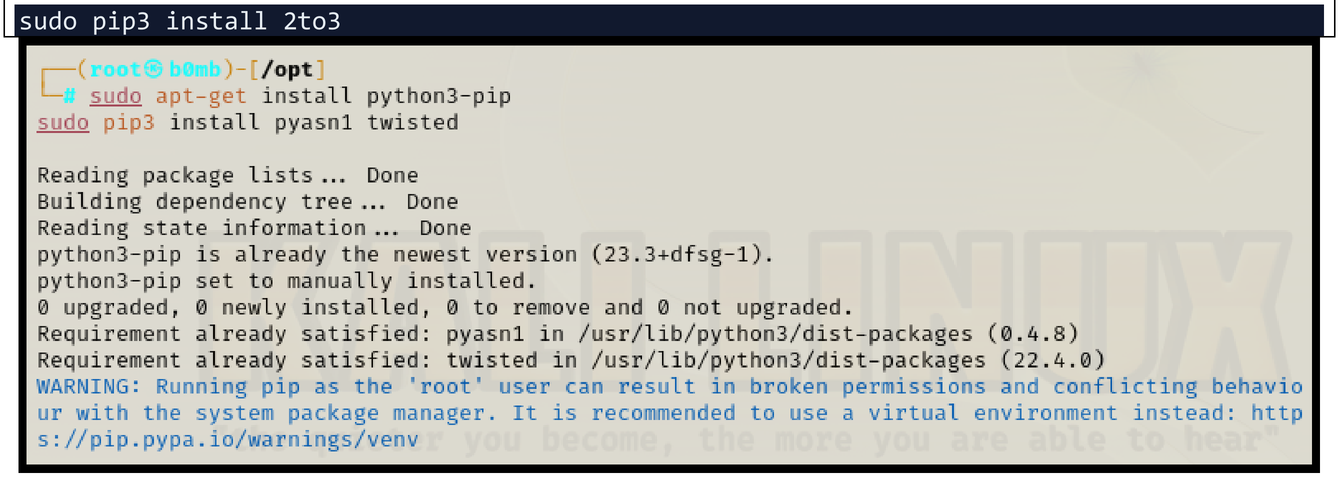


```
┌──(root㉿b0mb)-[/opt]
└─# sudo apt-get install python3-dev python3-openssl python3-pyasn1 python3-twisted

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3-dev is already the newest version (3.11.4-5+b1).
python3-dev set to manually installed.
python3-openssl is already the newest version (23.2.0-1).
python3-openssl set to manually installed.
python3-pyasn1 is already the newest version (0.4.8-4).
python3-pyasn1 set to manually installed.
python3-twisted is already the newest version (22.4.0-4).
python3-twisted set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

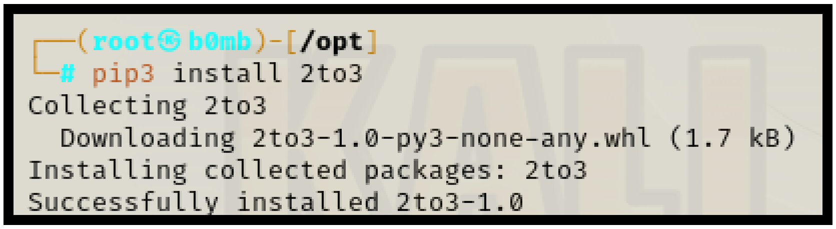
```
sudo apt-get install python3-pip
```

```
sudo pip3 install pyasn1 twisted
```

```
sudo pip3 install 2to3
```

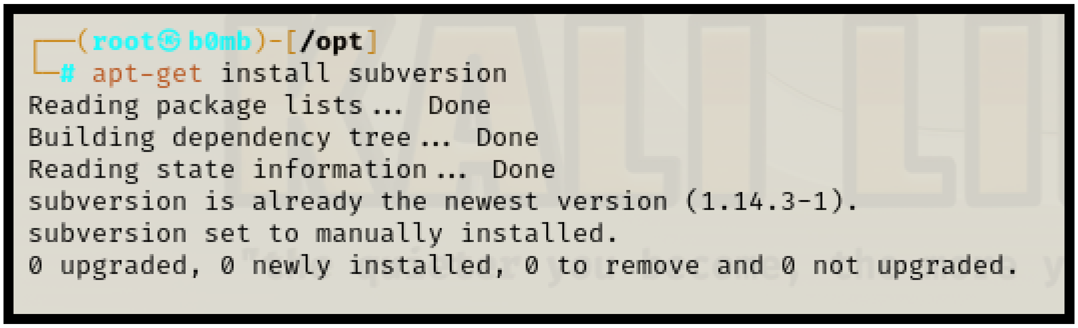


```
┌──(root㉿b0mb)-[/opt]
└─# sudo apt-get install python3-pip
sudo pip3 install pyasn1 twisted

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3-pip is already the newest version (23.3+dfsg-1).
python3-pip set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Requirement already satisfied: pyasn1 in /usr/lib/python3/dist-packages (0.4.8)
Requirement already satisfied: twisted in /usr/lib/python3/dist-packages (22.4.0)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behavio
ur with the system package manager. It is recommended to use a virtual environment instead: http
s://pip.pypa.io/warnings/venv
```



```
┌──(root㉿b0mb)-[/opt]
└─# pip3 install 2to3
Collecting 2to3
  Downloading 2to3-1.0-py3-none-any.whl (1.7 kB)
Installing collected packages: 2to3
Successfully installed 2to3-1.0
```

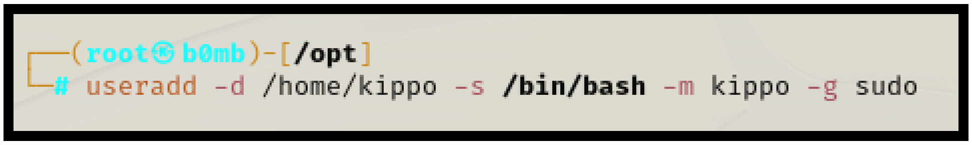
```
apt-get install subversion
```



```
┌──(root㉿b0mb)-[/opt]
└─# apt-get install subversion
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
subversion is already the newest version (1.14.3-1).
subversion set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Creating a Kippo user:-

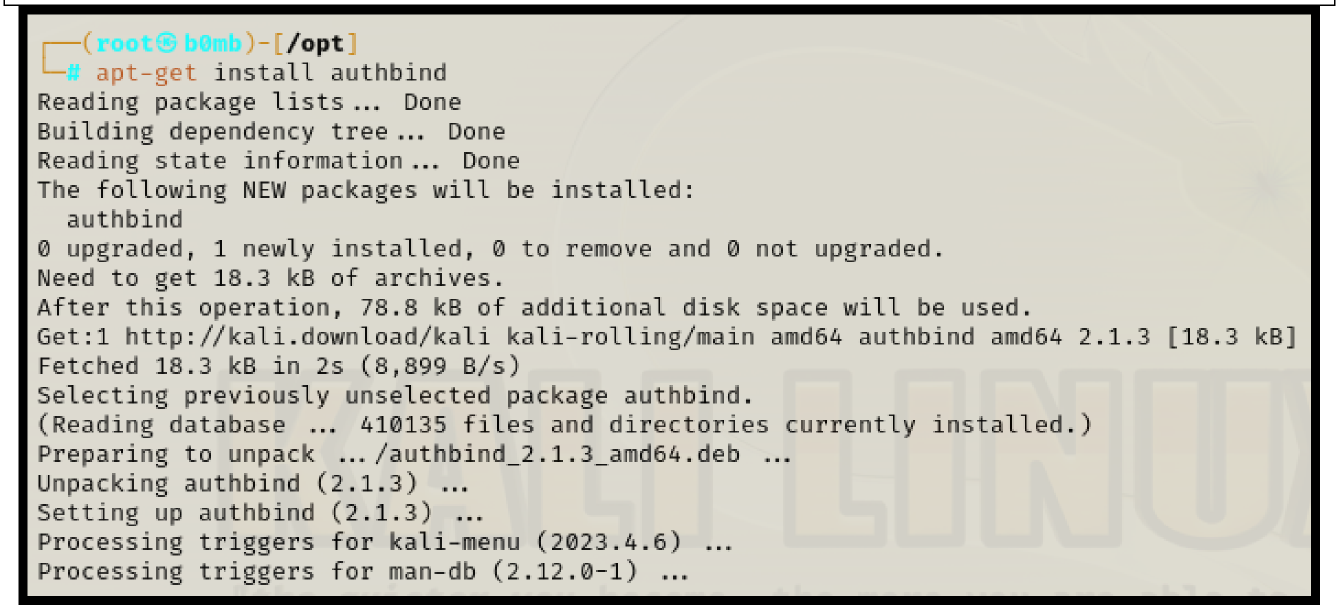
```
useradd -d /home/kippo -s /bin/bash -m kippo -g sudo
```



```
┌──(root㉿b0mb)-[/opt]
└─# useradd -d /home/kippo -s /bin/bash -m kippo -g sudo
```

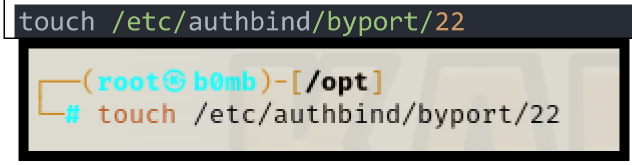
Installing AuthBind:

```
apt-get install authbind
```



```
┌──(root㉿b0mb)-[/opt]
└─# apt-get install authbind
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  authbind
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 18.3 kB of archives.
After this operation, 78.8 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 authbind amd64 2.1.3 [18.3 kB]
Fetched 18.3 kB in 2s (8,899 B/s)
Selecting previously unselected package authbind.
(Reading database ... 410135 files and directories currently installed.)
Preparing to unpack .../authbind_2.1.3_amd64.deb ...
Unpacking authbind (2.1.3) ...
Setting up authbind (2.1.3) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for man-db (2.12.0-1) ...
```

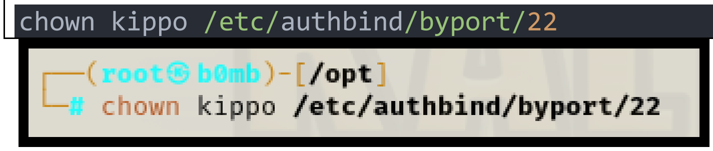
```
touch /etc/authbind/byport/22
```



```
┌──(root㉿b0mb)-[/opt]
└─# touch /etc/authbind/byport/22
```

Changing Ownership of the Kippo User: -

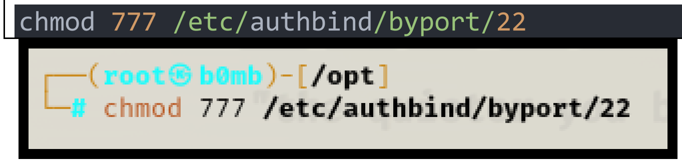
```
chown kippo /etc/authbind/byport/22
```



```
┌──(root㉿b0mb)-[/opt]
└─# chown kippo /etc/authbind/byport/22
```

Changing the Permissions: -

```
chmod 777 /etc/authbind/byport/22
```



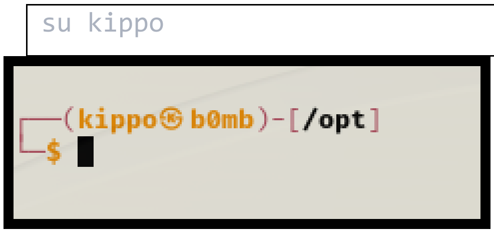
```
┌──(root㉿b0mb)-[/opt]
└─# chmod 777 /etc/authbind/byport/22
```

Downloading the Kippo Honeypot : -

https://github.com/desaster/kippo

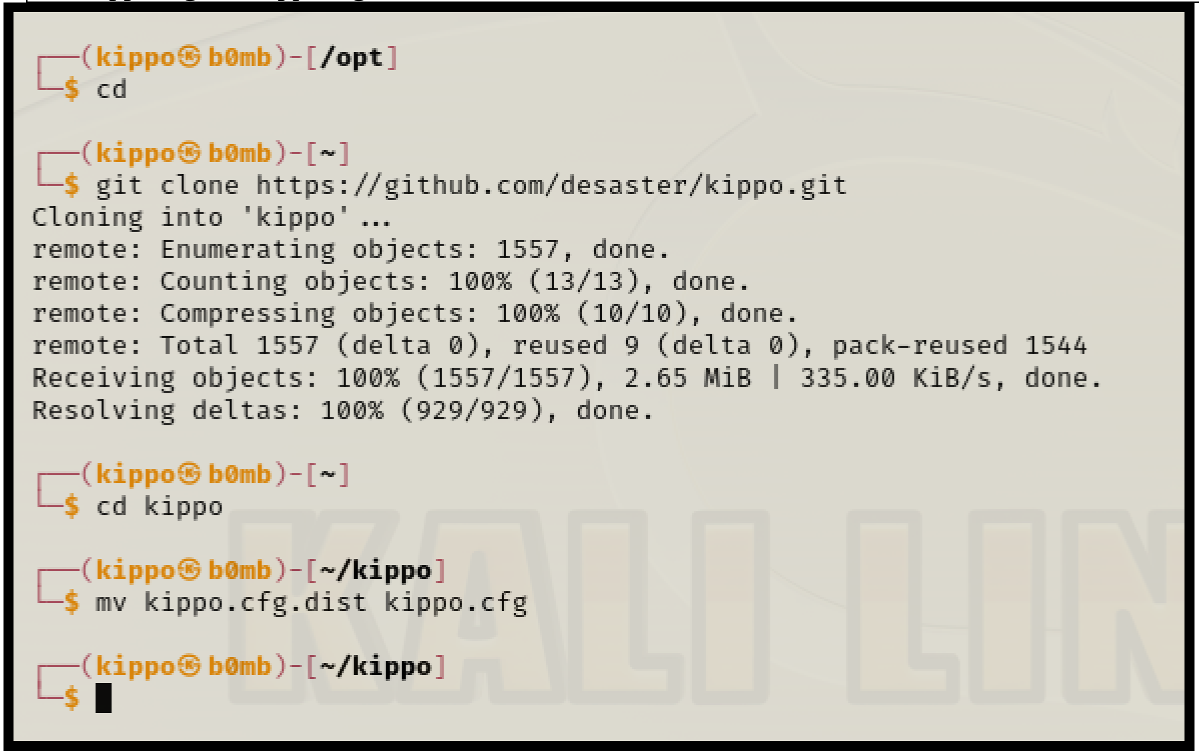
Using the Kippo User

```
su kippo
```



```
┌──(kippo㉿b0mb)-[/opt]
└─$ 
```

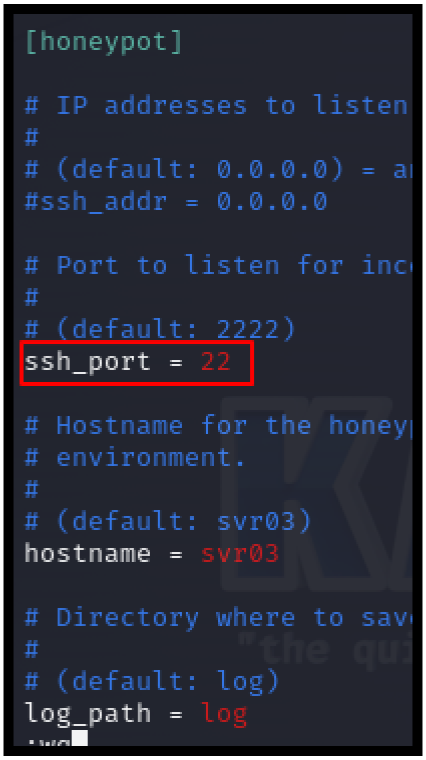
```
cd
git clone https://github.com/desaster/kippo.git
cd kippo
mv kippo.cfg.dist kippo.cfg
```



```
┌──(kippo㉿b0mb)-[/opt]
└─$ cd

┌──(kippo㉿b0mb)-[~]
└─$ git clone https://github.com/desaster/kippo.git
Cloning into 'kippo'...
remote: Enumerating objects: 1557, done.
remote: Counting objects: 100% (13/13), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 1557 (delta 0), reused 9 (delta 0), pack-reused 1544
Receiving objects: 100% (1557/1557), 2.65 MiB | 335.00 KiB/s, done.
Resolving deltas: 100% (929/929), done.

┌──(kippo㉿b0mb)-[~]
└─$ cd kippo

┌──(kippo㉿b0mb)-[~/kippo]
└─$ mv kippo.cfg.dist kippo.cfg

┌──(kippo㉿b0mb)-[~/kippo]
└─$ 
```

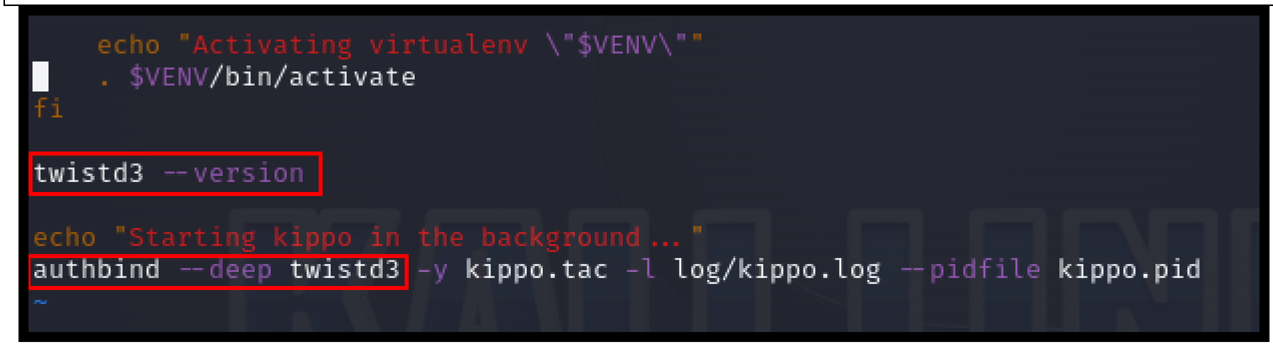
Configuring Kippo:-

```
vi kippo.cfg
```



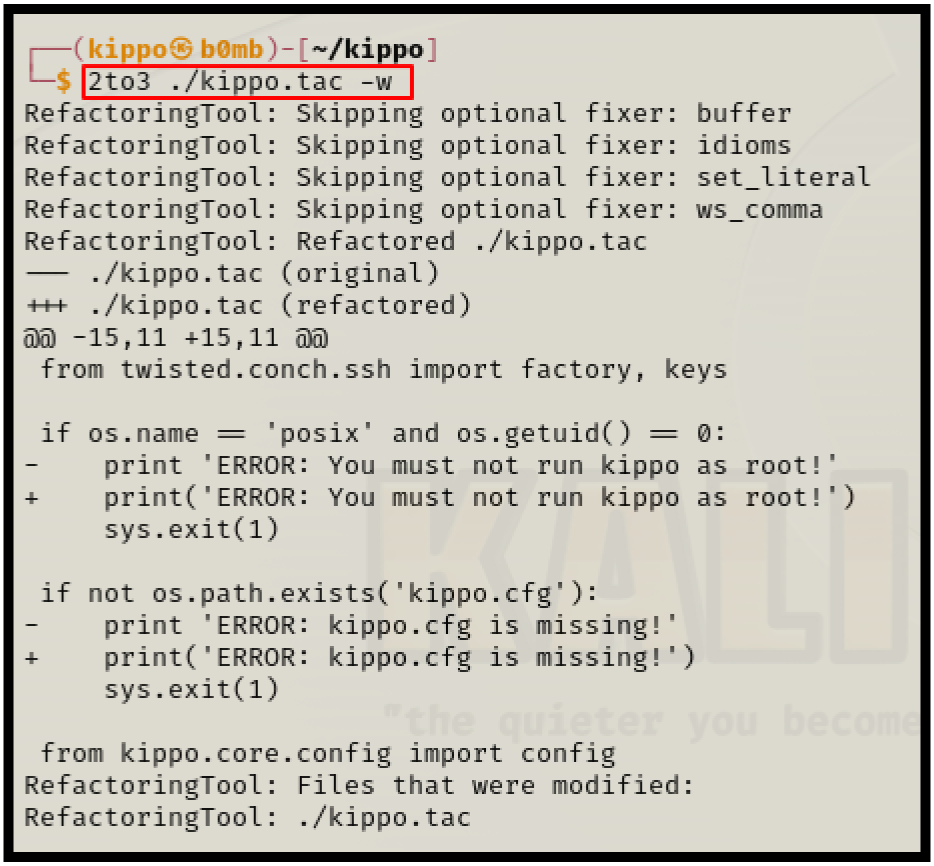
```
[honeypot]

# IP addresses to listen
#
# (default: 0.0.0.0) = a
#ssh_addr = 0.0.0.0

# Port to listen for inc
#
# (default: 2222)
ssh_port = 22

# Hostname for the honey
# environment.
#
# (default: svr03)
hostname = svr03

# Directory where to sav
#
# (default: log)
log_path = log
:wq
```

vi start.sh



```
    echo "Activating virtualenv \"$VENV\""
    . $VENV/bin/activate
fi

twistd3 --version

echo "Starting kippo in the background..."
authbind --deep twistd3 -y kippo.tac -l log/kippo.log --pidfile kippo.pid
~
```

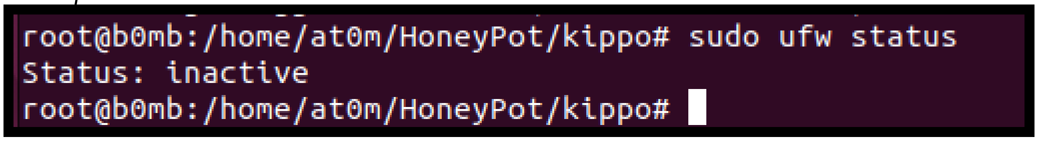
2to3 ./kippo.tac -w



```
┌──(kippo㉿b0mb)-[~/kippo]
└─$ 2to3 ./kippo.tac -w
RefactoringTool: Skipping optional fixer: buffer
RefactoringTool: Skipping optional fixer: idioms
RefactoringTool: Skipping optional fixer: set_literal
RefactoringTool: Skipping optional fixer: ws_comma
RefactoringTool: Refactored ./kippo.tac
--- ./kippo.tac (original)
+++ ./kippo.tac (refactored)
@@ -15,11 +15,11 @@
 from twisted.conch.ssh import factory, keys

 if os.name == 'posix' and os.getuid() == 0:
-    print 'ERROR: You must not run kippo as root!'
+    print('ERROR: You must not run kippo as root!')
     sys.exit(1)

 if not os.path.exists('kippo.cfg'):
-    print 'ERROR: kippo.cfg is missing!'
+    print('ERROR: kippo.cfg is missing!')
     sys.exit(1)

 from kippo.core.config import config
RefactoringTool: Files that were modified:
RefactoringTool: ./kippo.tac
```

Configure Firewall Rules for SSH

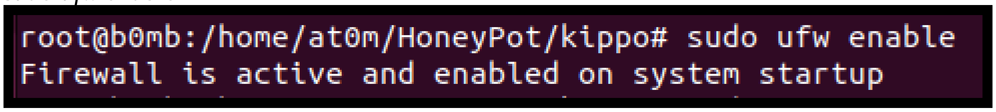
sudo ufw status



```
root@b0mb:/home/at0m/HoneyPot/kippo# sudo ufw status
Status: inactive
root@b0mb:/home/at0m/HoneyPot/kippo# █
```

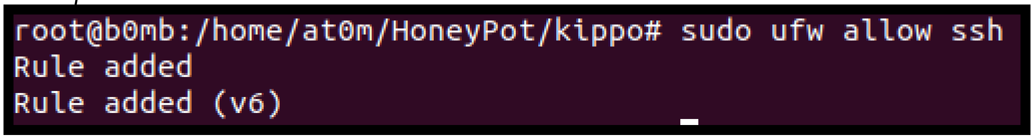
IF INACTIVE

sudo ufw enable



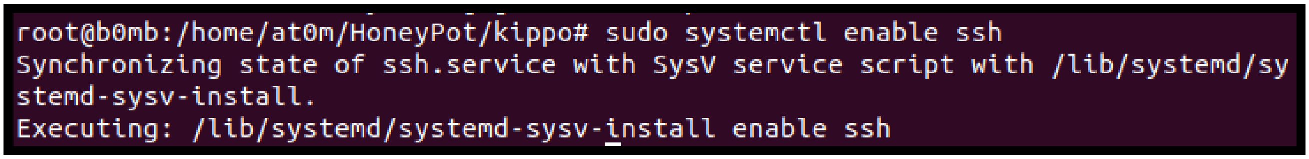
```
root@b0mb:/home/at0m/HoneyPot/kippo# sudo ufw enable
Firewall is active and enabled on system startup
```

sudo ufw allow ssh

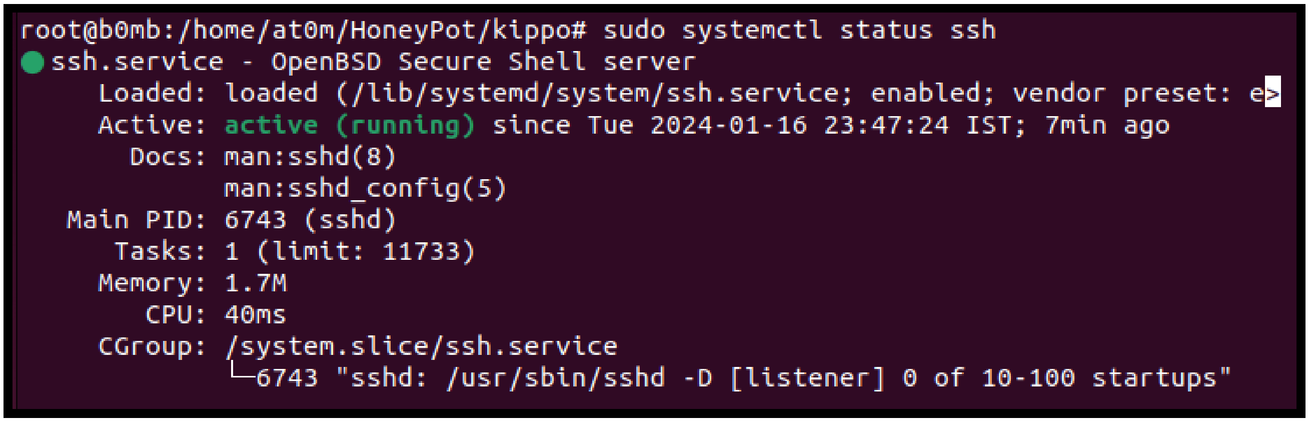


```
root@b0mb:/home/at0m/HoneyPot/kippo# sudo ufw allow ssh
Rule added
Rule added (v6)
```

Enabling SSH On Startup



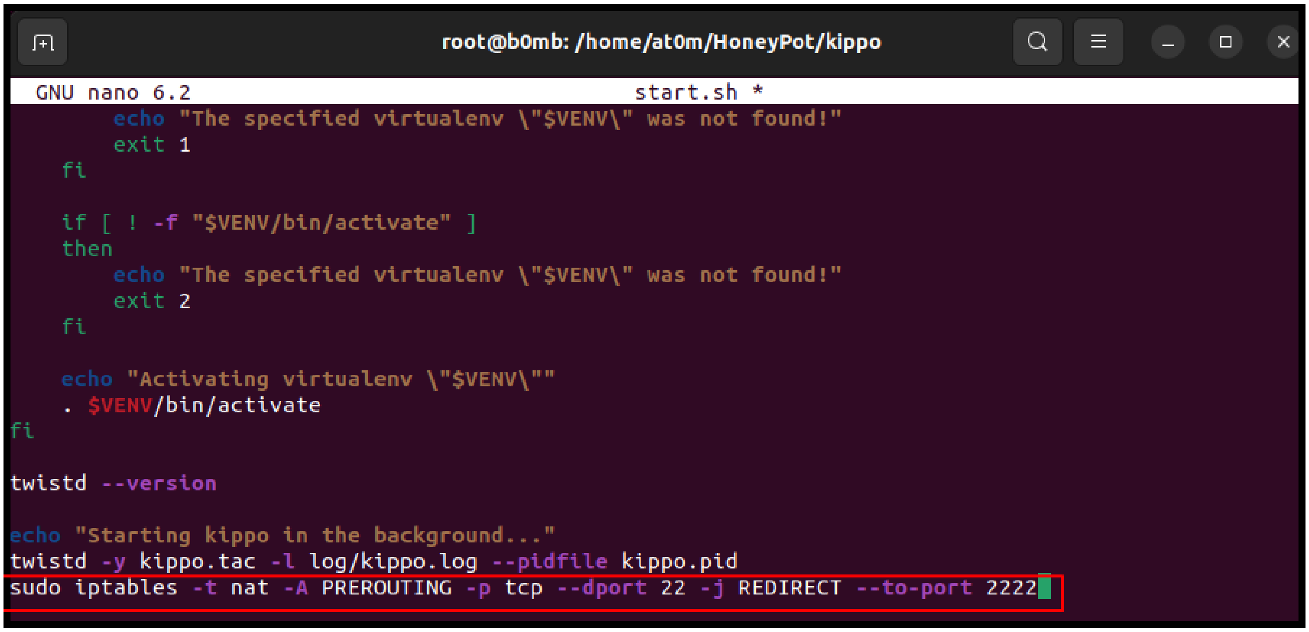
```
root@b0mb:/home/at0m/HoneyPot/kippo# sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
```



```
root@b0mb:/home/at0m/HoneyPot/kippo# sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e>
     Active: active (running) since Tue 2024-01-16 23:47:24 IST; 7min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 6743 (sshd)
      Tasks: 1 (limit: 11733)
     Memory: 1.7M
        CPU: 40ms
     CGroup: /system.slice/ssh.service
             └─6743 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

Editing the start.sh file (Port Forwarding)

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 22 
-j REDIRECT --to-port 2222
```



root@b0mb: /home/at0m/HoneyPot/kippo

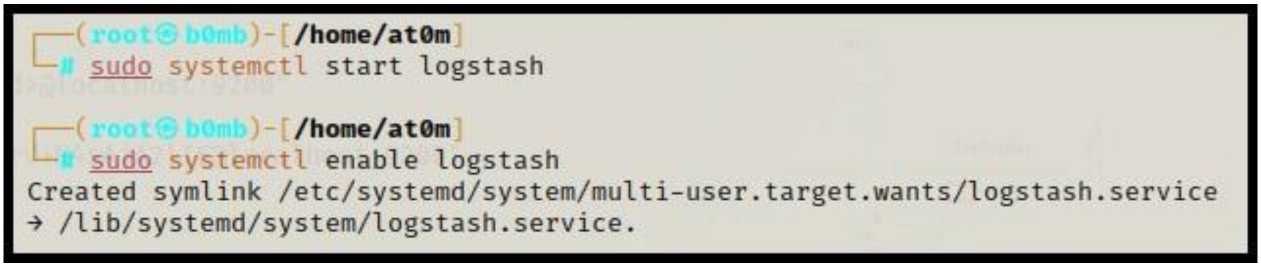
```
  GNU nano 6.2                                          start.sh *
            echo "The specified virtualenv \"$VENV\" was not found!"
            exit 1
        fi

        if [ ! -f "$VENV/bin/activate" ]
        then
            echo "The specified virtualenv \"$VENV\" was not found!"
            exit 2
        fi

        echo "Activating virtualenv \"$VENV\""
        . $VENV/bin/activate
fi

twistd --version

echo "Starting kippo in the background..."
twistd -y kippo.tac -l log/kippo.log --pidfile kippo.pid
sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port 2222
```

Starting and Enabling Logstash Service

Command: -

```
sudo systemctl start logstash.service
```

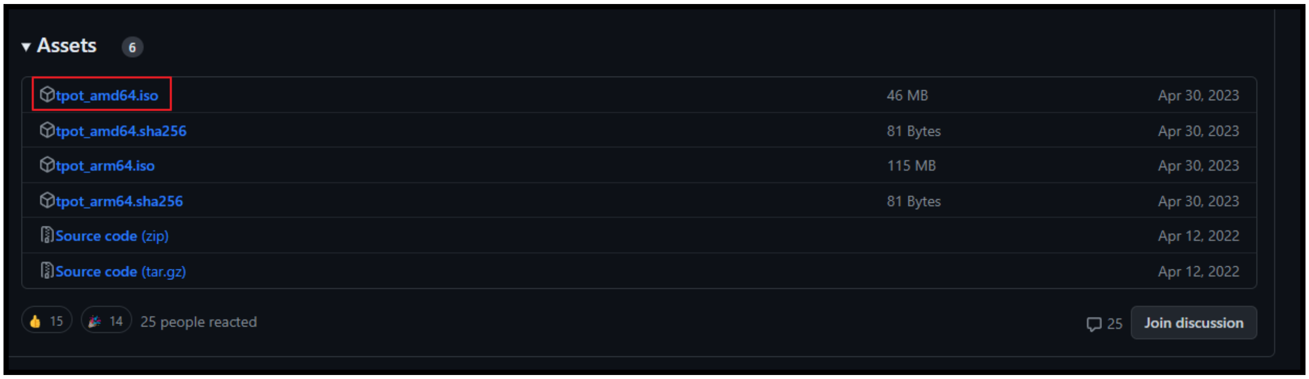
```
sudo systemctl enable logstash.service
```



```
┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl start logstash

┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service
→ /lib/systemd/system/logstash.service.
```

Download T-POT ISO

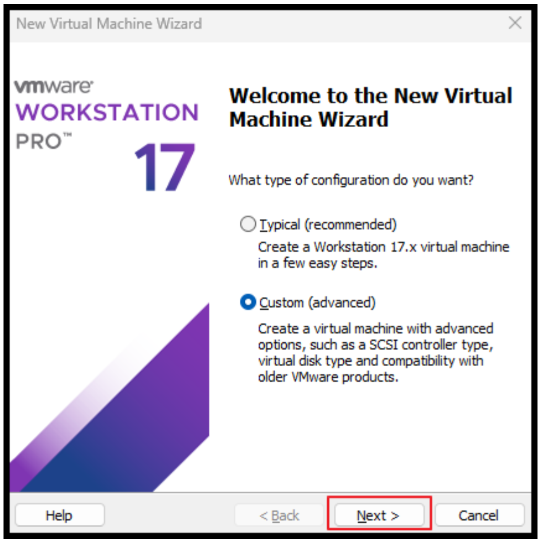
https://github.com/telekom-security/tpotce/releases



▾ Assets 6

tpot_amd64.iso	46 MB	Apr 30, 2023
tpot_amd64.sha256	81 Bytes	Apr 30, 2023
tpot_arm64.iso	115 MB	Apr 30, 2023
tpot_arm64.sha256	81 Bytes	Apr 30, 2023
Source code (zip)		Apr 12, 2022
Source code (tar.gz)		Apr 12, 2022

Making a new VM from T-POT ISO (VMware Pro)



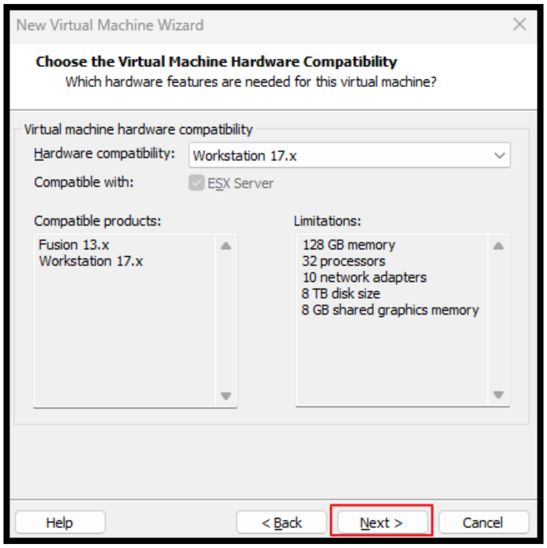
New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

○ Typical (recommended)
Create a Workstation 17.x virtual machine in a few easy steps.

● Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.



New Virtual Machine Wizard

Choose the Virtual Machine Hardware Compatibility

Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility

Hardware compatibility: Workstation 17.x

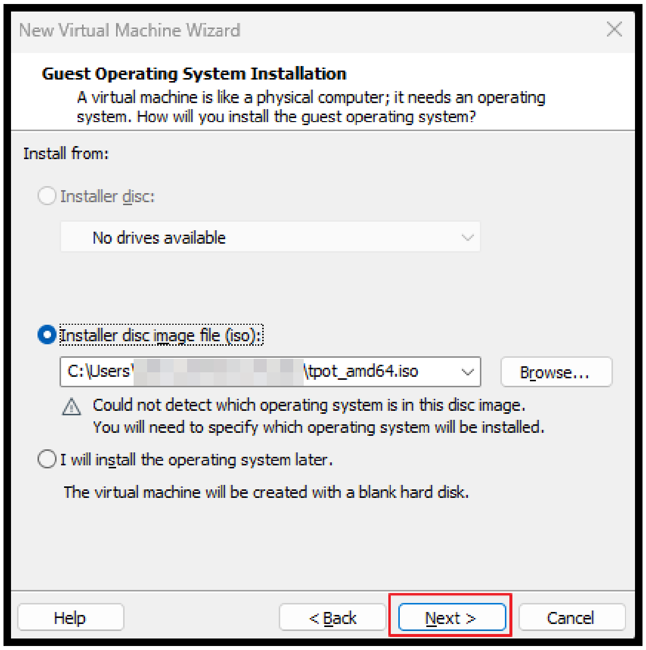
Compatible with: ☑ ESX Server

Compatible products:

Fusion 13.x
Workstation 17.x

Limitations:

128 GB memory
32 processors
10 network adapters
8 TB disk size
8 GB shared graphics memory



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

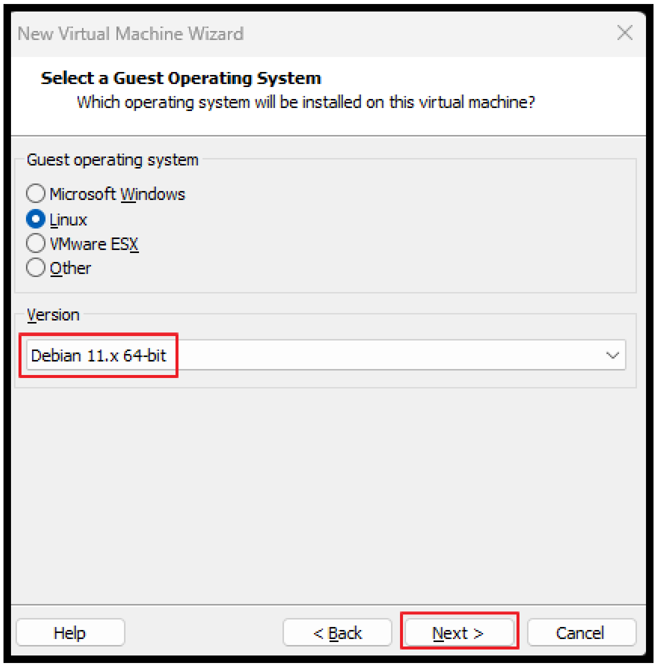
● Installer disc image file (iso):

C:\Users\[redacted]\tpot_amd64.iso

⚠ Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.



New Virtual Machine Wizard

Select a Guest Operating System

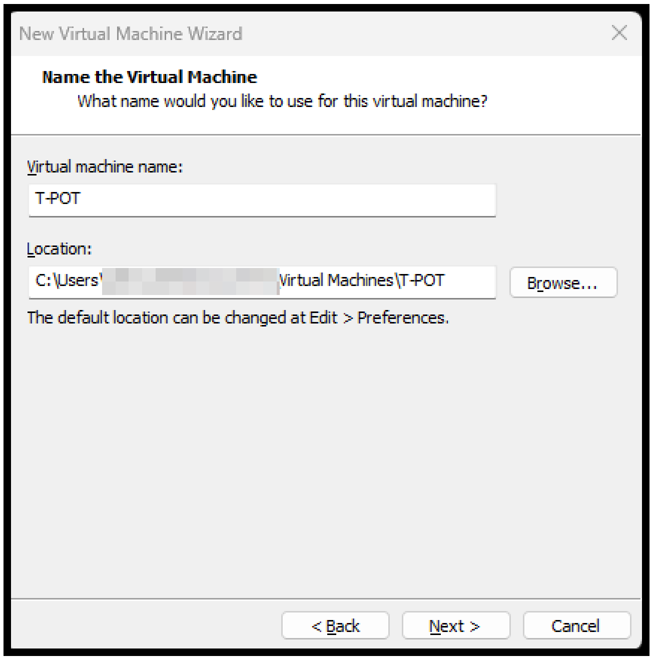
Which operating system will be installed on this virtual machine?

Guest operating system

○ Microsoft Windows
● Linux
○ VMware ESX
○ Other

Version

Debian 11.x 64-bit



New Virtual Machine Wizard

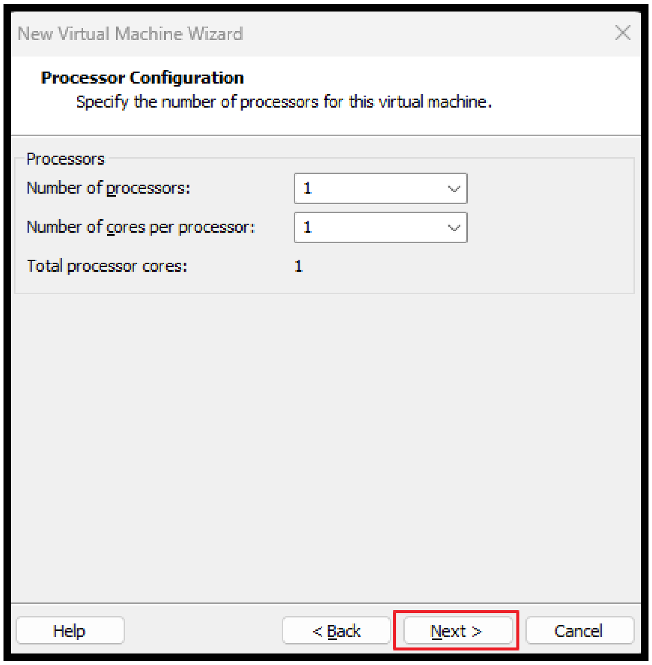
Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name: T-POT

Location: C:\Users\[redacted]\Virtual Machines\T-POT

The default location can be changed at Edit > Preferences.



New Virtual Machine Wizard

Processor Configuration

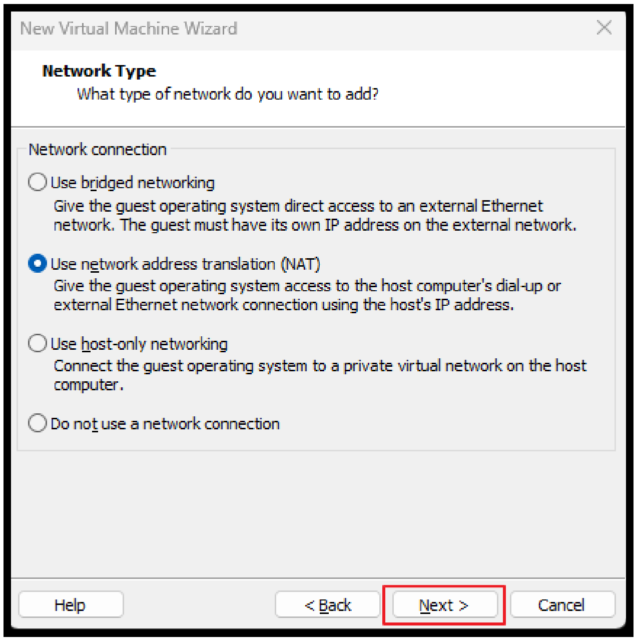
Specify the number of processors for this virtual machine.

Processors

Number of processors: 1

Number of cores per processor: 1

Total processor cores: 1



New Virtual Machine Wizard

Network Type

What type of network do you want to add?

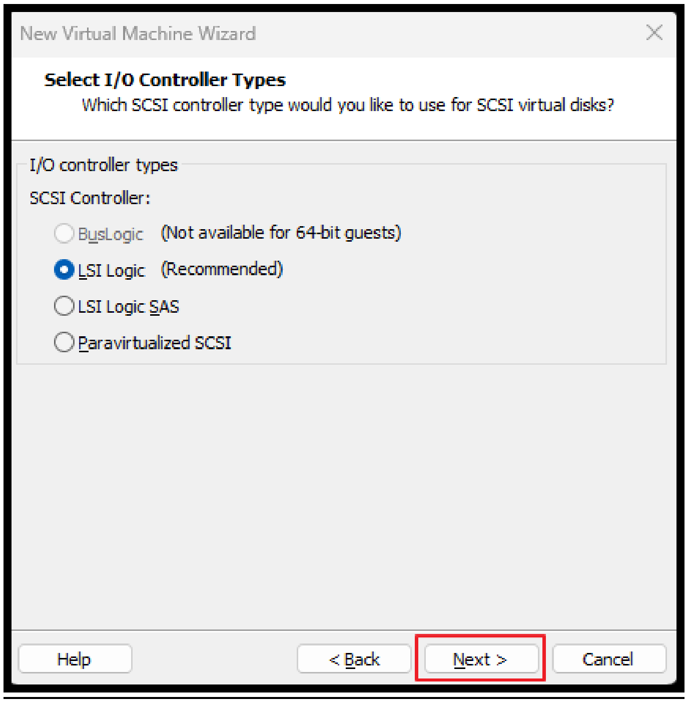
Network connection

○ Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

● Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

○ Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.

○ Do not use a network connection



New Virtual Machine Wizard

Select I/O Controller Types

Which SCSI controller type would you like to use for SCSI virtual disks?

I/O controller types

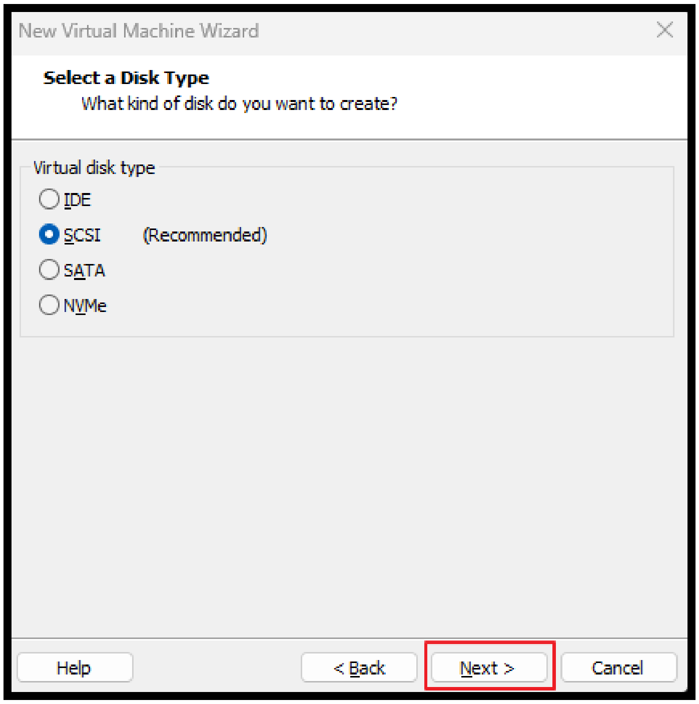
SCSI Controller:

○ BusLogic (Not available for 64-bit guests)

● LSI Logic (Recommended)

○ LSI Logic SAS

○ Paravirtualized SCSI



New Virtual Machine Wizard

Select a Disk Type

What kind of disk do you want to create?

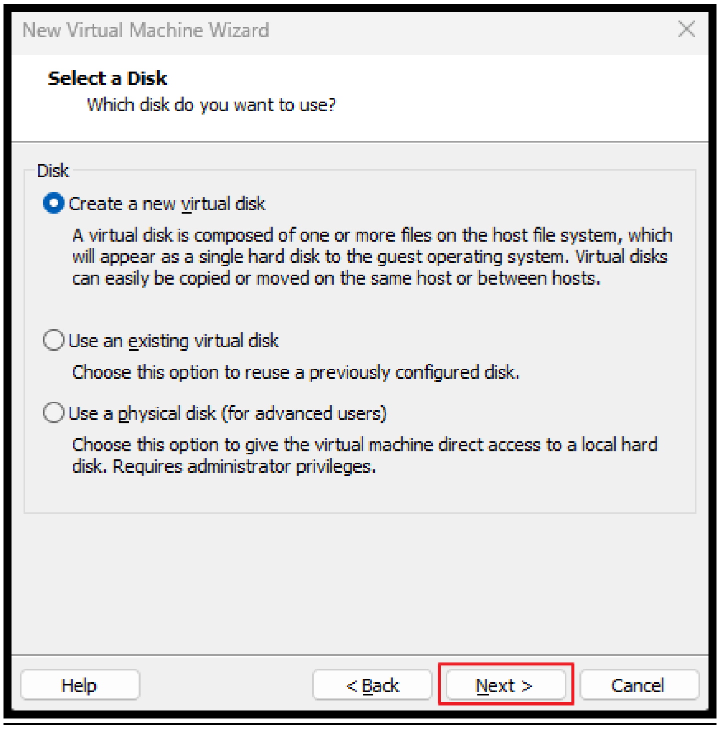
Virtual disk type

○ IDE

● SCSI (Recommended)

○ SATA

○ NVMe



New Virtual Machine Wizard

Select a Disk

Which disk do you want to use?

Disk

● Create a new virtual disk

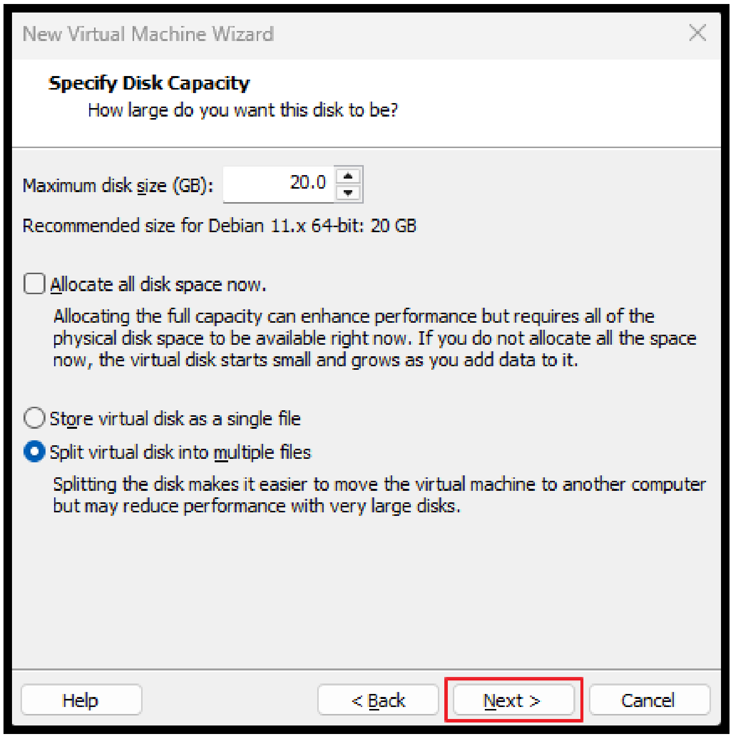
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

○ Use an existing virtual disk

Choose this option to reuse a previously configured disk.

○ Use a physical disk (for advanced users)

Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB): 20.0

Recommended size for Debian 11.x 64-bit: 20 GB

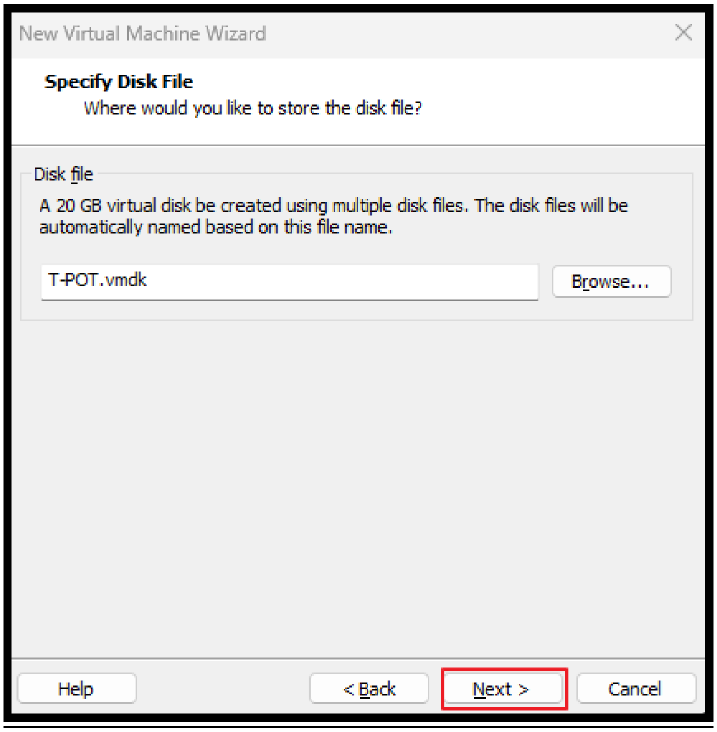
□ Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.



New Virtual Machine Wizard

Specify Disk File

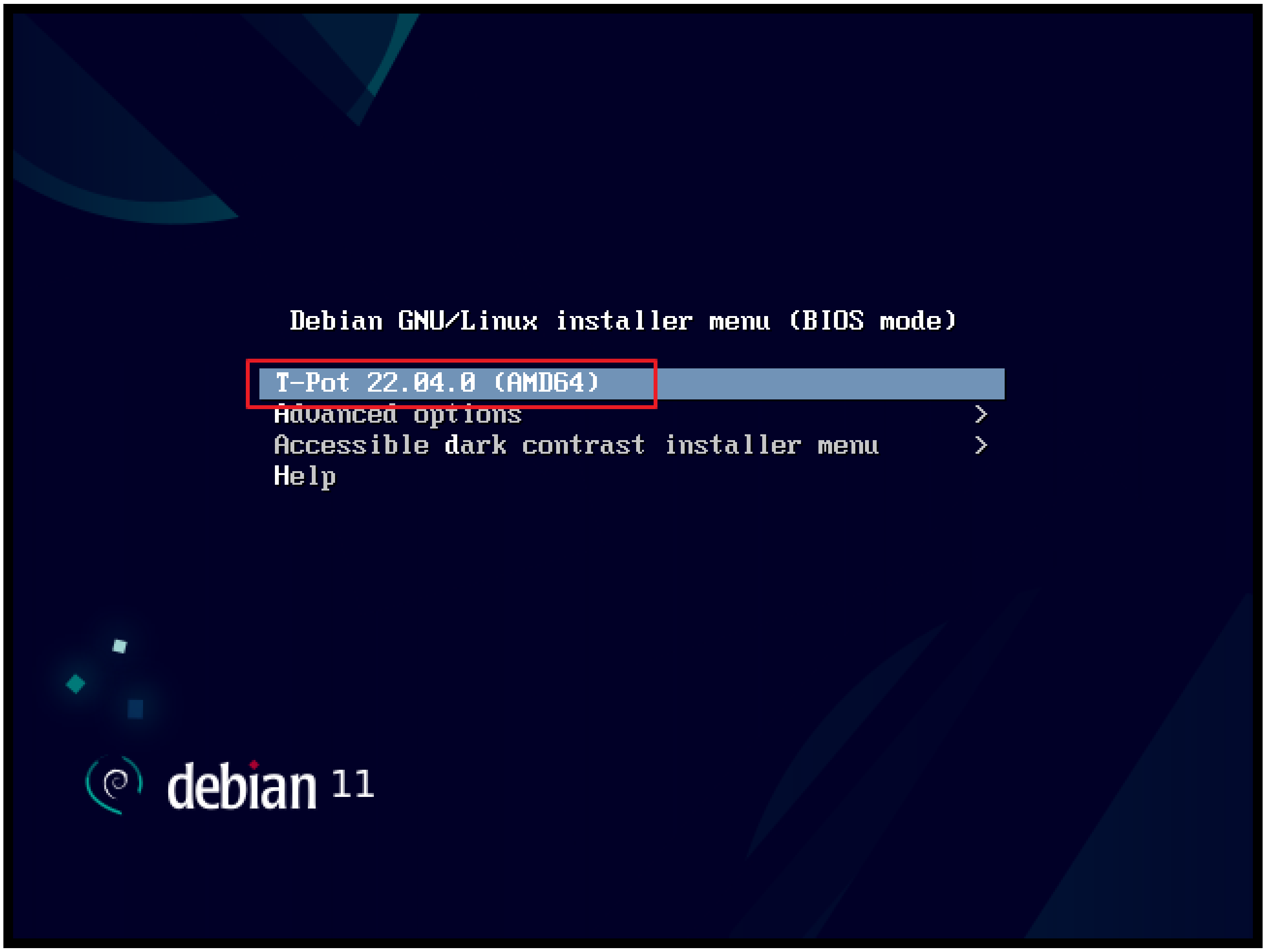
Where would you like to store the disk file?

Disk file

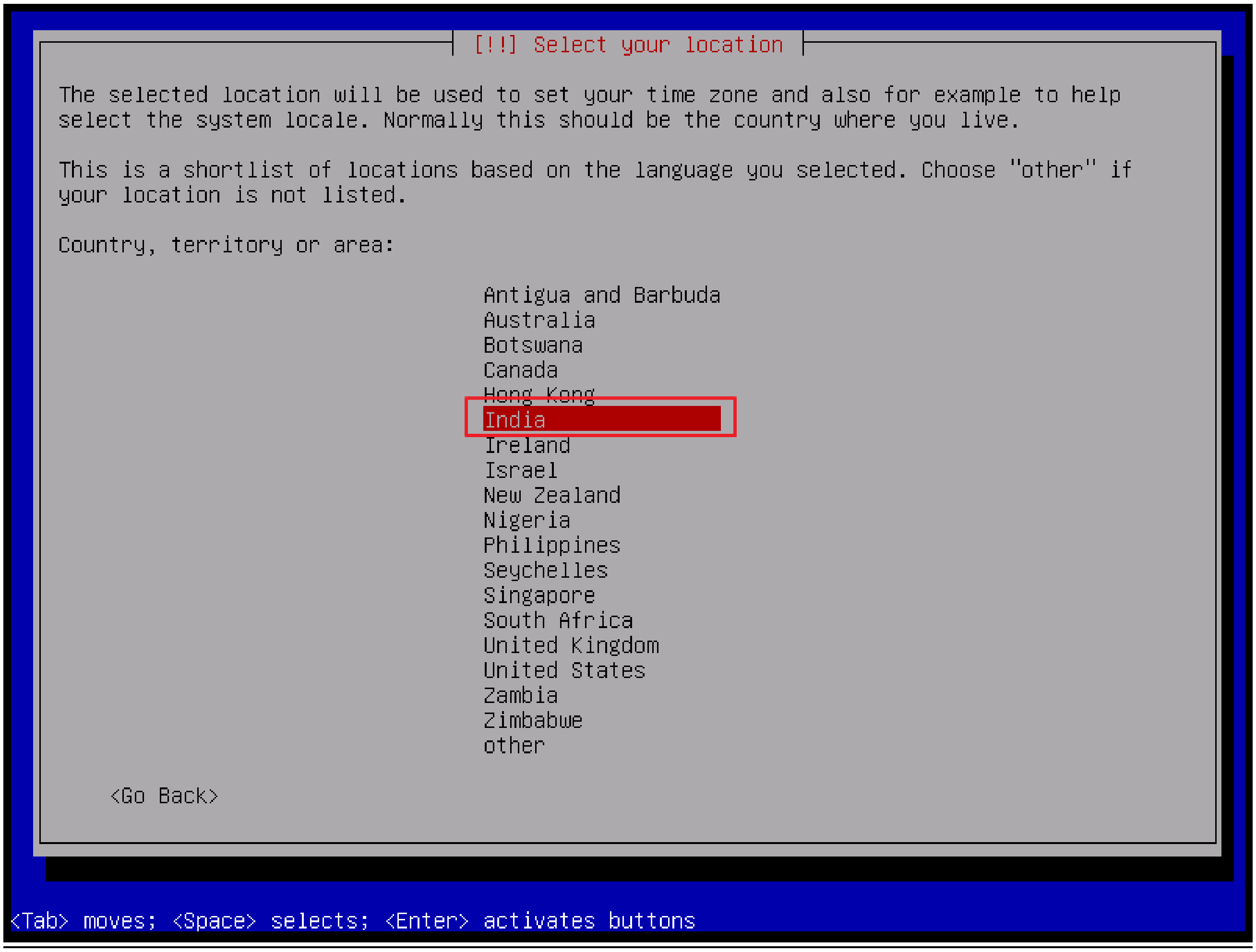
A 20 GB virtual disk be created using multiple disk files. The disk files will be automatically named based on this file name.

T-POT.vmdk

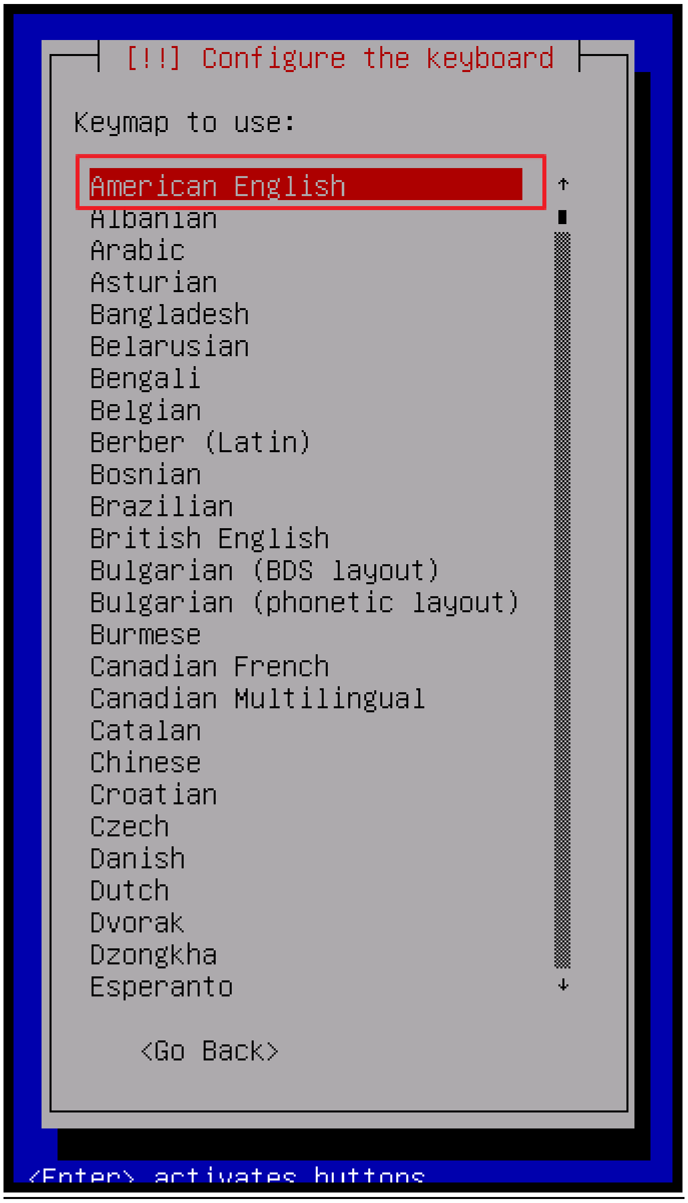
Installing T-POT ISO (VMware Pro)



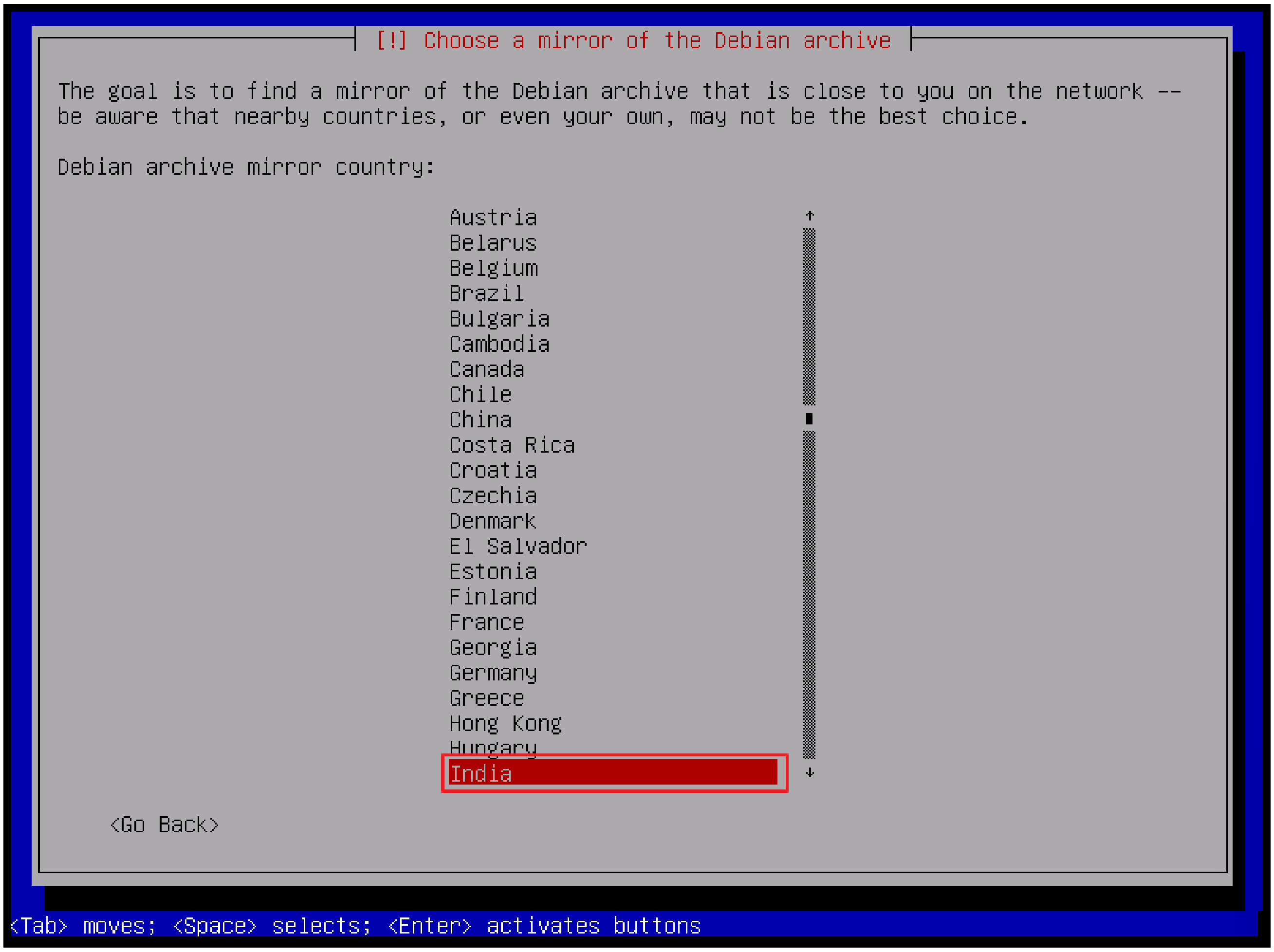
```
Debian GNU/Linux installer menu (BIOS mode)

T-Pot 22.04.0 (AMD64)
Advanced options                               >
Accessible dark contrast installer menu        >
Help
```



```
[!!] Select your location

The selected location will be used to set your time zone and also for example to help
select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if
your location is not listed.

Country, territory or area:

                                  Antigua and Barbuda
                                  Australia
                                  Botswana
                                  Canada
                                  Hong Kong
                                  India
                                  Ireland
                                  Israel
                                  New Zealand
                                  Nigeria
                                  Philippines
                                  Seychelles
                                  Singapore
                                  South Africa
                                  United Kingdom
                                  United States
                                  Zambia
                                  Zimbabwe
                                  other

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```
]



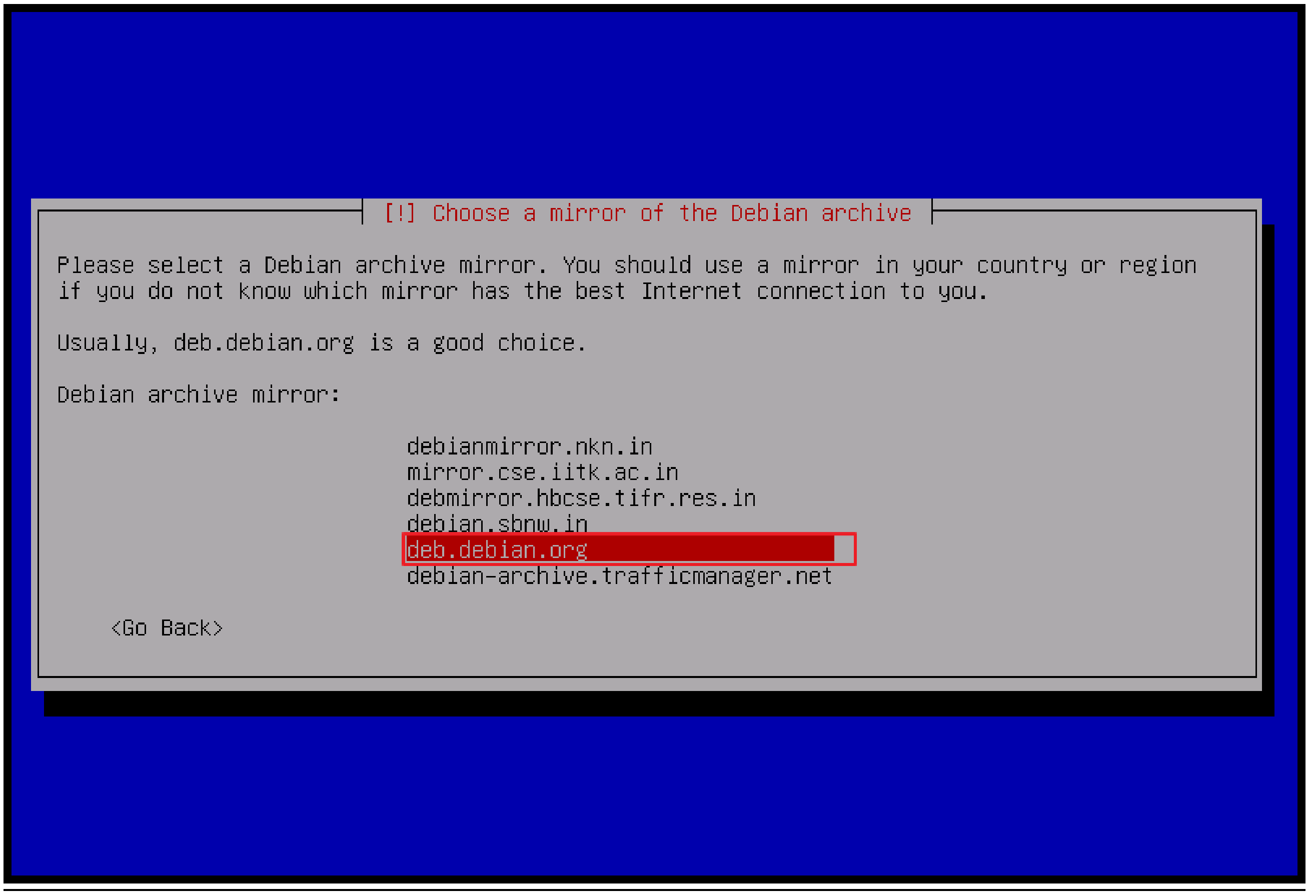
```
[!!] Configure the keyboard

Keymap to use:

  American English
  Albanian
  Arabic
  Asturian
  Bangladesh
  Belarusian
  Bengali
  Belgian
  Berber (Latin)
  Bosnian
  Brazilian
  British English
  Bulgarian (BDS layout)
  Bulgarian (phonetic layout)
  Burmese
  Canadian French
  Canadian Multilingual
  Catalan
  Chinese
  Croatian
  Czech
  Danish
  Dutch
  Dvorak
  Dzongkha
  Esperanto

     <Go Back>

<Enter> activates buttons
```



[!] Choose a mirror of the Debian archive

The goal is to find a mirror of the Debian archive that is close to you on the network -- be aware that nearby countries, or even your own, may not be the best choice.

Debian archive mirror country:

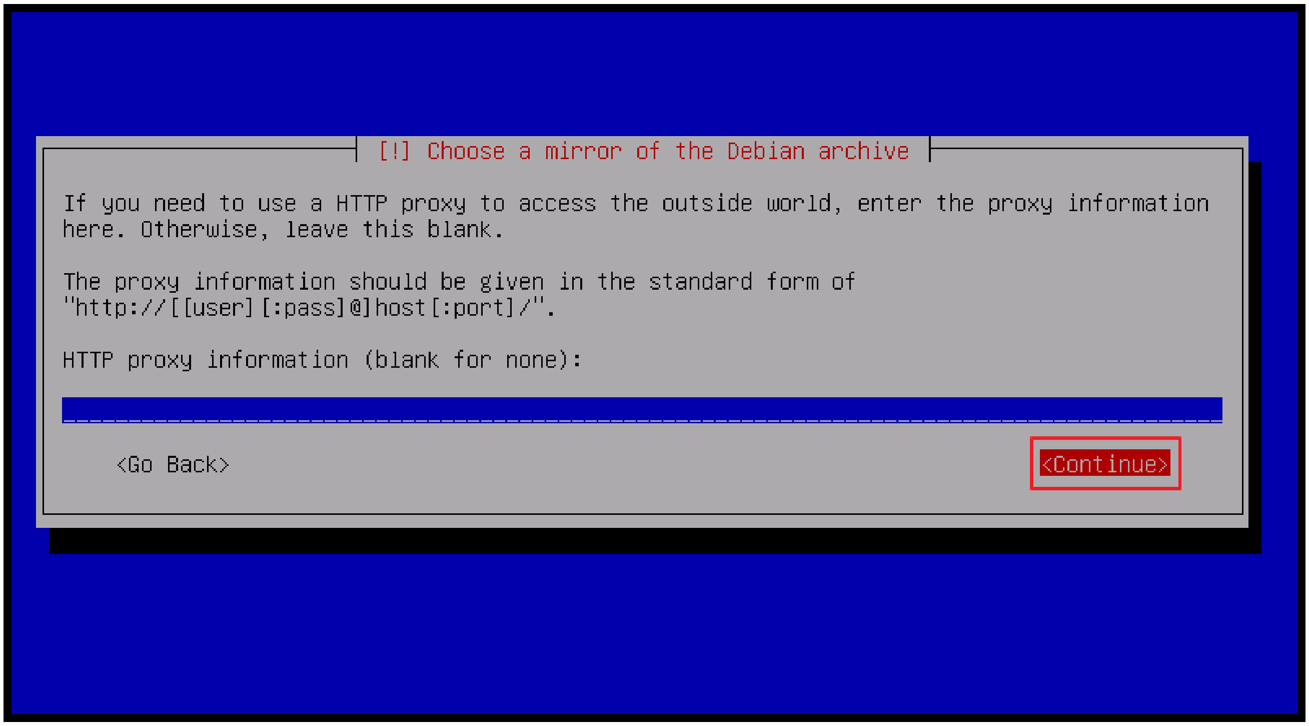


[!] Choose a mirror of the Debian archive

Please select a Debian archive mirror. You should use a mirror in your country or region if you do not know which mirror has the best Internet connection to you.

Usually, deb.debian.org is a good choice.

Debian archive mirror:

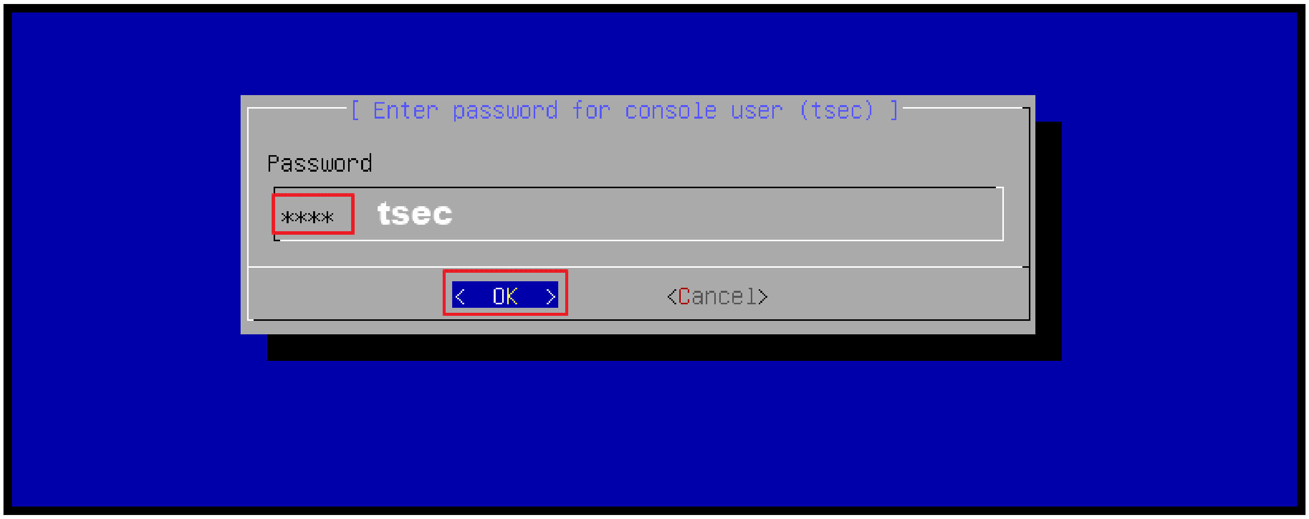


[!] Choose a mirror of the Debian archive

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".

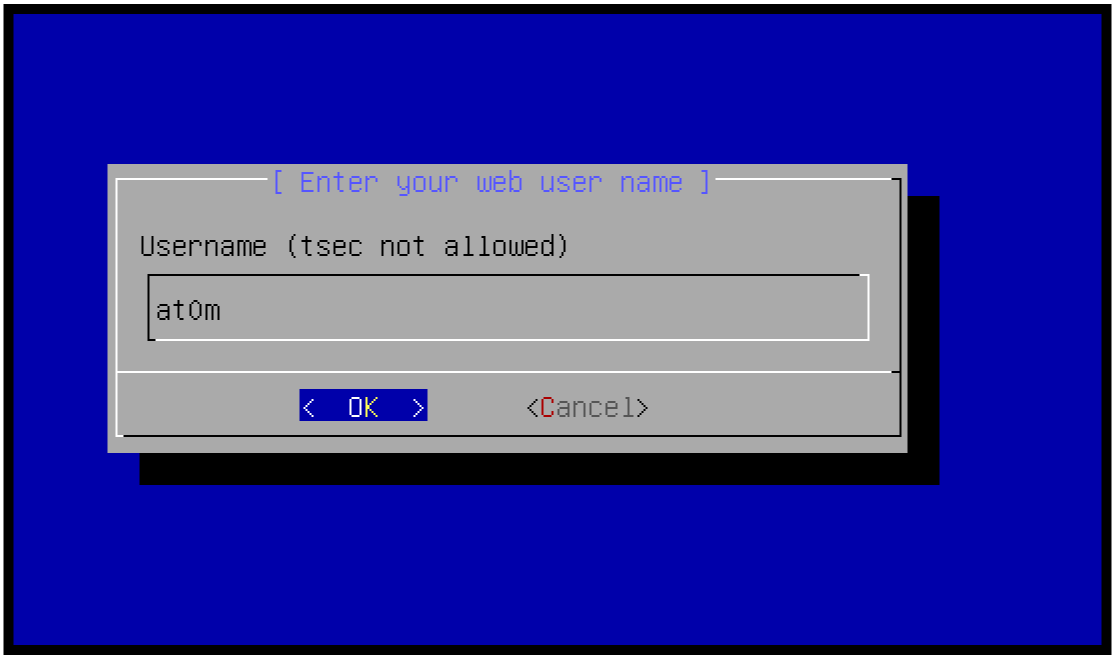
HTTP proxy information (blank for none):



[Enter password for console user (tsec)]

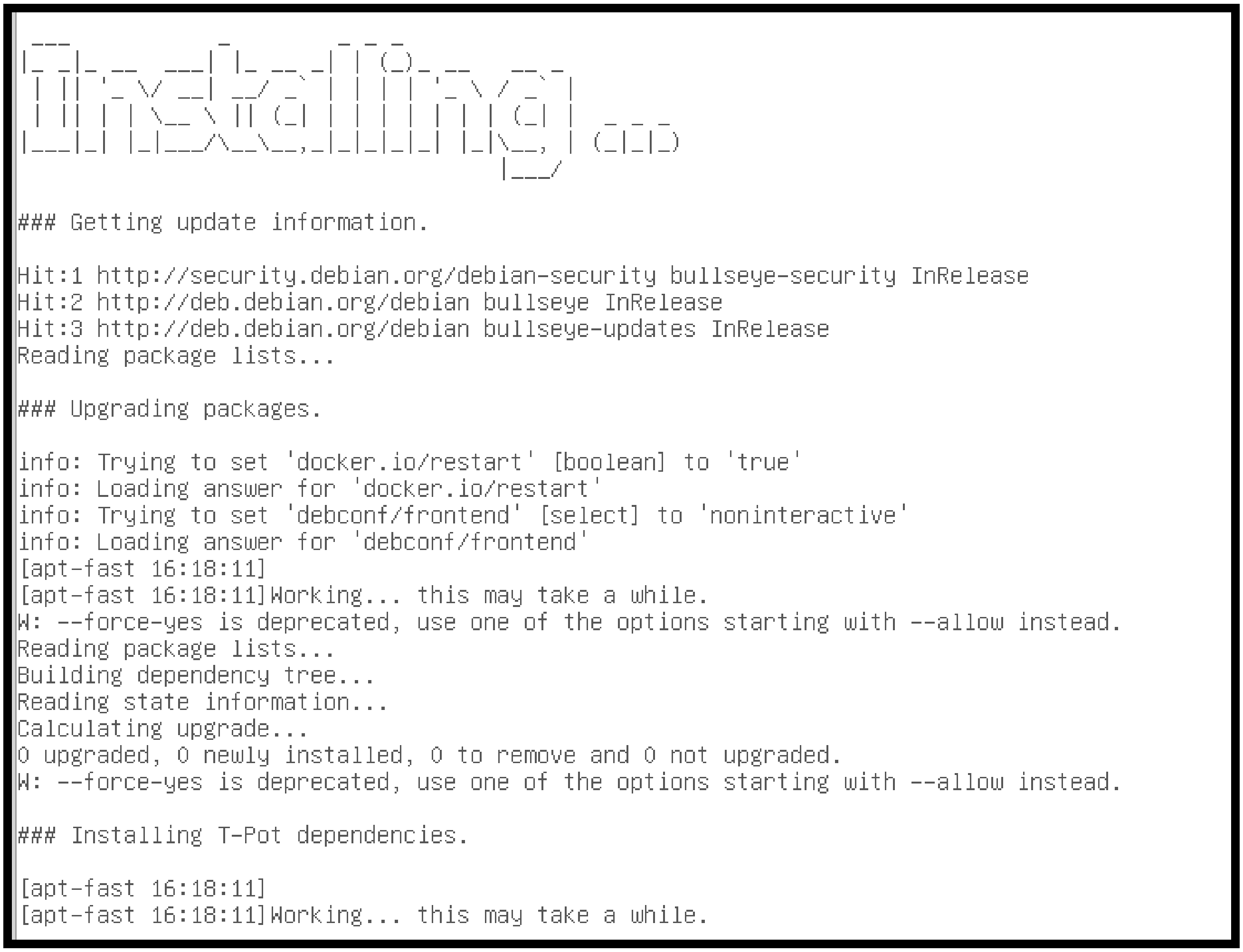
Password

****

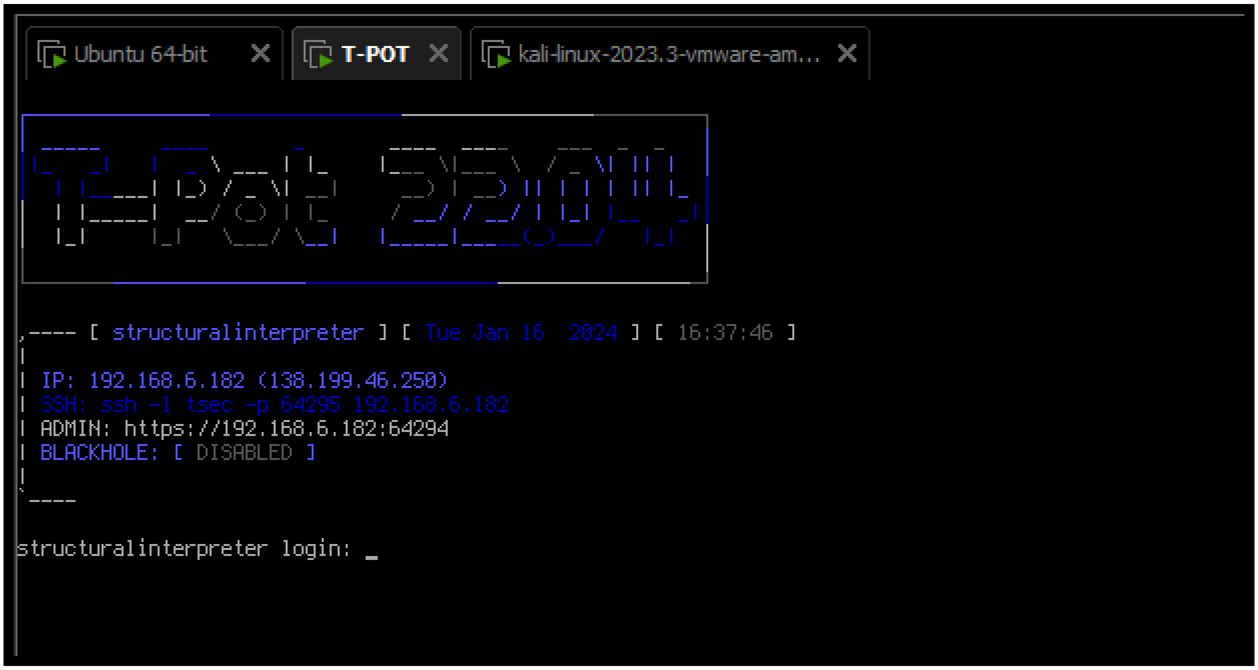


Username (tsec not allowed)

at0m



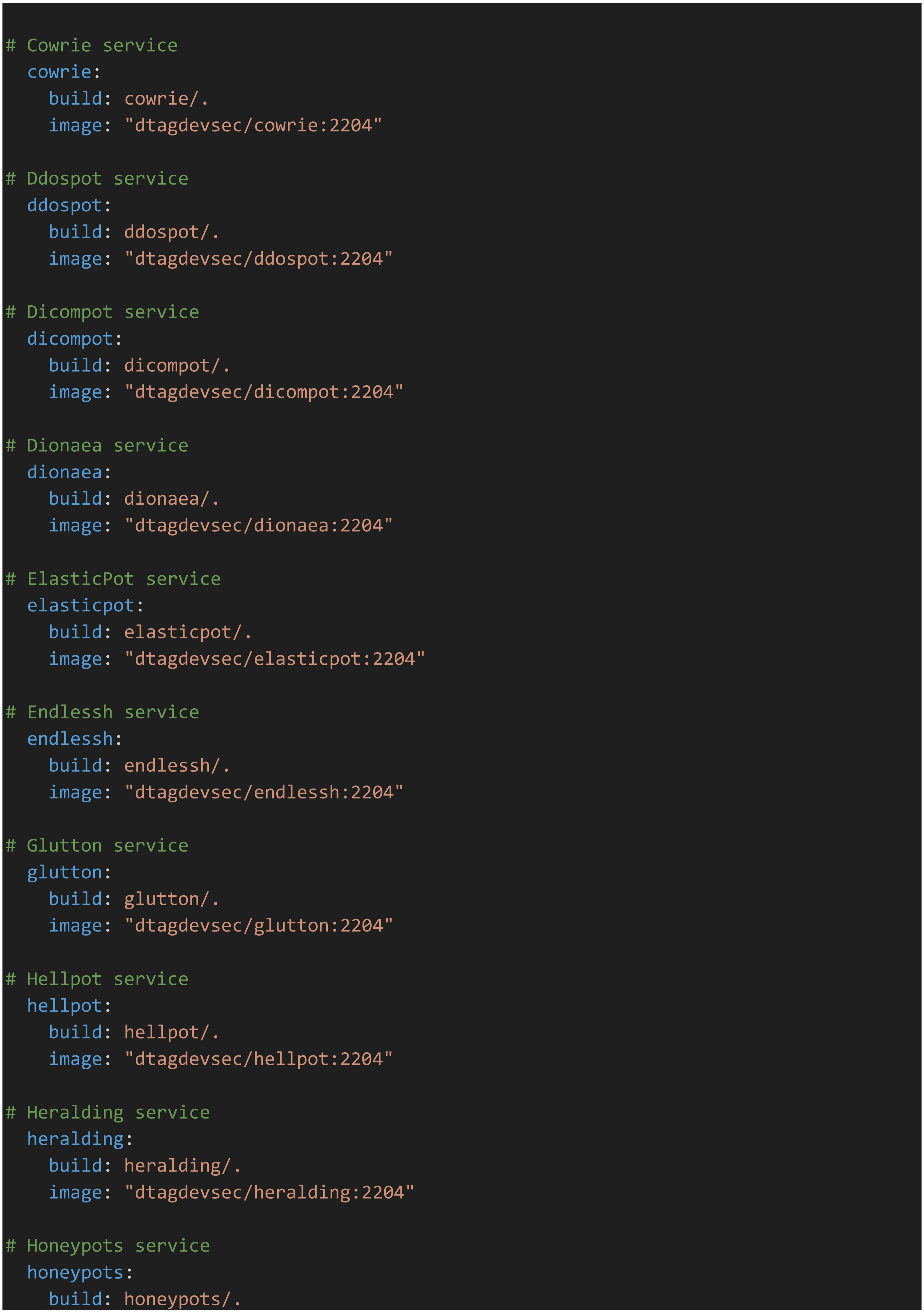
```
 ___           _        _ _ _
|_ _|_ __  ___| |_ __ _| | (_)_ __   __ _
 | || '_ \/ __| __/ _` | | | | '_ \ / _` |
 | || | | \__ \ || (_| | | | | | | | (_| | _ _ _
|___|_| |_|___/\__\__,_|_|_|_|_| |_|\__, | (_|_|_)
                                    |___/

### Getting update information.

Hit:1 http://security.debian.org/debian-security bullseye-security InRelease
Hit:2 http://deb.debian.org/debian bullseye InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Reading package lists...

### Upgrading packages.

info: Trying to set 'docker.io/restart' [boolean] to 'true'
info: Loading answer for 'docker.io/restart'
info: Trying to set 'debconf/frontend' [select] to 'noninteractive'
info: Loading answer for 'debconf/frontend'
[apt-fast 16:18:11]
[apt-fast 16:18:11]Working... this may take a while.
W: --force-yes is deprecated, use one of the options starting with --allow instead.
Reading package lists...
Building dependency tree...
Reading state information...
Calculating upgrade...
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
W: --force-yes is deprecated, use one of the options starting with --allow instead.

### Installing T-Pot dependencies.

[apt-fast 16:18:11]
[apt-fast 16:18:11]Working... this may take a while.
```



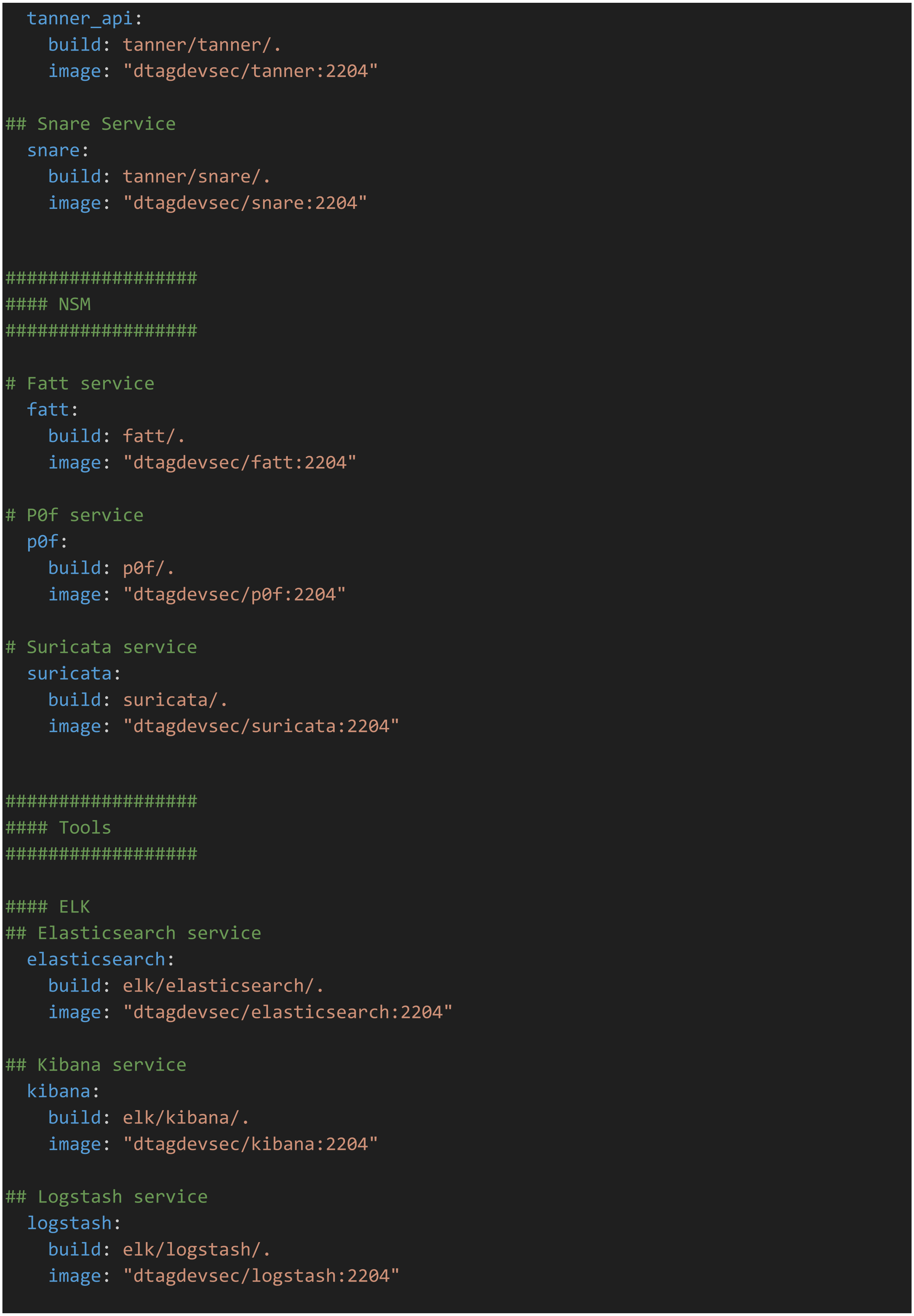
```
,---- [ structuralinterpreter ] [ Tue Jan 16  2024 ] [ 16:37:46 ]
|
| IP: 192.168.6.182 (138.199.46.250)
| SSH: ssh -l tsec -p 64295 192.168.6.182
| ADMIN: https://192.168.6.182:64294
| BLACKHOLE: [ DISABLED ]
|
`----

structuralinterpreter login: _
```

Docker Configuarations

```
# T-Pot Image Builder (use only for building docker images)
version: '2.3'

services:

##################
#### Honeypots
##################

# Adbhoney service
  adbhoney:
    build: adbhoney/.
    image: "dtagdevsec/adbhoney:2204"

# Ciscoasa service
  ciscoasa:
    build: ciscoasa/.
    image: "dtagdevsec/ciscoasa:2204"

# CitrixHoneypot service
  citrixhoneypot:
    build: citrixhoneypot/.
    image: "dtagdevsec/citrixhoneypot:2204"

# Conpot IEC104 service
  conpot_IEC104:
    build: conpot/.
    image: "dtagdevsec/conpot:2204"
```



```
# Cowrie service
  cowrie:
    build: cowrie/.
    image: "dtagdevsec/cowrie:2204"

# Ddospot service
  ddospot:
    build: ddospot/.
    image: "dtagdevsec/ddospot:2204"

# Dicompot service
  dicompot:
    build: dicompot/.
    image: "dtagdevsec/dicompot:2204"

# Dionaea service
  dionaea:
    build: dionaea/.
    image: "dtagdevsec/dionaea:2204"

# ElasticPot service
  elasticpot:
    build: elasticpot/.
    image: "dtagdevsec/elasticpot:2204"

# Endlessh service
  endlessh:
    build: endlessh/.
    image: "dtagdevsec/endlessh:2204"

# Glutton service
  glutton:
    build: glutton/.
    image: "dtagdevsec/glutton:2204"

# Hellpot service
  hellpot:
    build: hellpot/.
    image: "dtagdevsec/hellpot:2204"

# Heralding service
  heralding:
    build: heralding/.
    image: "dtagdevsec/heralding:2204"

# Honeypots service
  honeypots:
    build: honeypots/.
    image: "dtagdevsec/honeypots:2204"

# Honeytrap service
  honeytrap:
    build: honeytrap/.
    image: "dtagdevsec/honeytrap:2204"

# IPPHoney service
  ipphoney:
    build: ipphoney/.
    image: "dtagdevsec/ipphoney:2204"

# Log4Pot service
  log4pot:
    build: log4pot/.
    image: "dtagdevsec/log4pot:2204"

# Mailoney service
  mailoney:
    build: mailoney/.
    image: "dtagdevsec/mailoney:2204"

# Medpot service
  medpot:
    build: medpot/.
    image: "dtagdevsec/medpot:2204"

# Redishoneypot service
  redishoneypot:
    build: redishoneypot/.
    image: "dtagdevsec/redishoneypot:2204"

# Sentrypeer service
  sentrypeer:
    build: sentrypeer/.
    image: "dtagdevsec/sentrypeer:2204"

#### Snare / Tanner
## Tanner Redis Service
  tanner_redis:
    build: tanner/redis/.
    image: "dtagdevsec/redis:2204"

## PHP Sandbox service
  tanner_phpox:
    build: tanner/phpox/.
    image: "dtagdevsec/phpox:2204"

## Tanner API Service
```



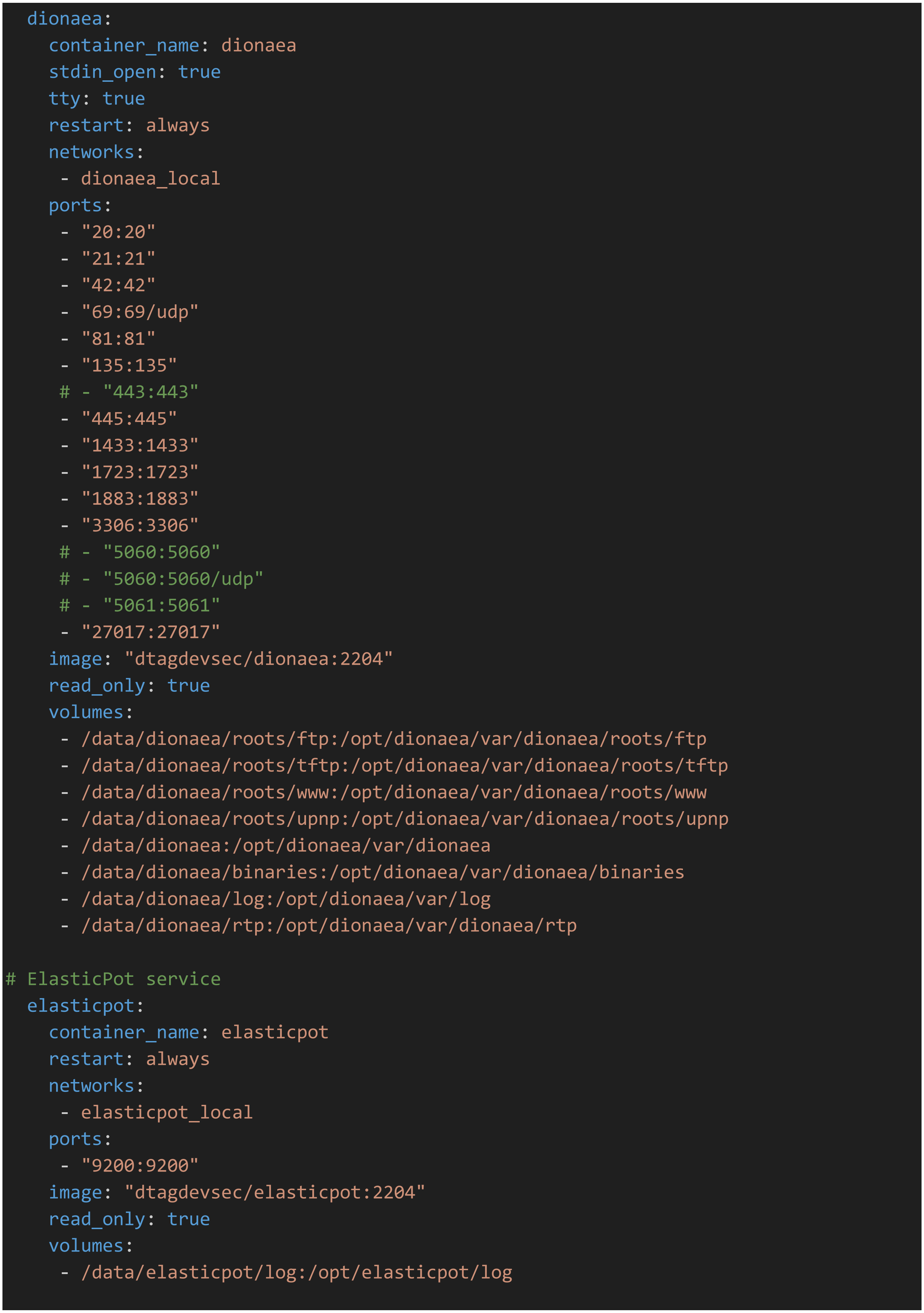
```
  tanner_api:
    build: tanner/tanner/.
    image: "dtagdevsec/tanner:2204"

## Snare Service
  snare:
    build: tanner/snare/.
    image: "dtagdevsec/snare:2204"


##################
#### NSM
##################

# Fatt service
  fatt:
    build: fatt/.
    image: "dtagdevsec/fatt:2204"

# P0f service
  p0f:
    build: p0f/.
    image: "dtagdevsec/p0f:2204"

# Suricata service
  suricata:
    build: suricata/.
    image: "dtagdevsec/suricata:2204"


##################
#### Tools
##################

#### ELK
## Elasticsearch service
  elasticsearch:
    build: elk/elasticsearch/.
    image: "dtagdevsec/elasticsearch:2204"

## Kibana service
  kibana:
    build: elk/kibana/.
    image: "dtagdevsec/kibana:2204"

## Logstash service
  logstash:
    build: elk/logstash/.
    image: "dtagdevsec/logstash:2204"
```

```
# Ewsposter service
  ewsposter:
    build: ewsposter/.
    image: "dtagdevsec/ewsposter:2204"

# Nginx service
  nginx:
    build: nginx/.
    image: "dtagdevsec/nginx:2204"

# Spiderfoot service
  spiderfoot:
    build: spiderfoot/.
    image: "dtagdevsec/spiderfoot:2204"

# Map Web Service
  map_web:
    build: elk/map/.
    image: "dtagdevsec/map:2204"
```

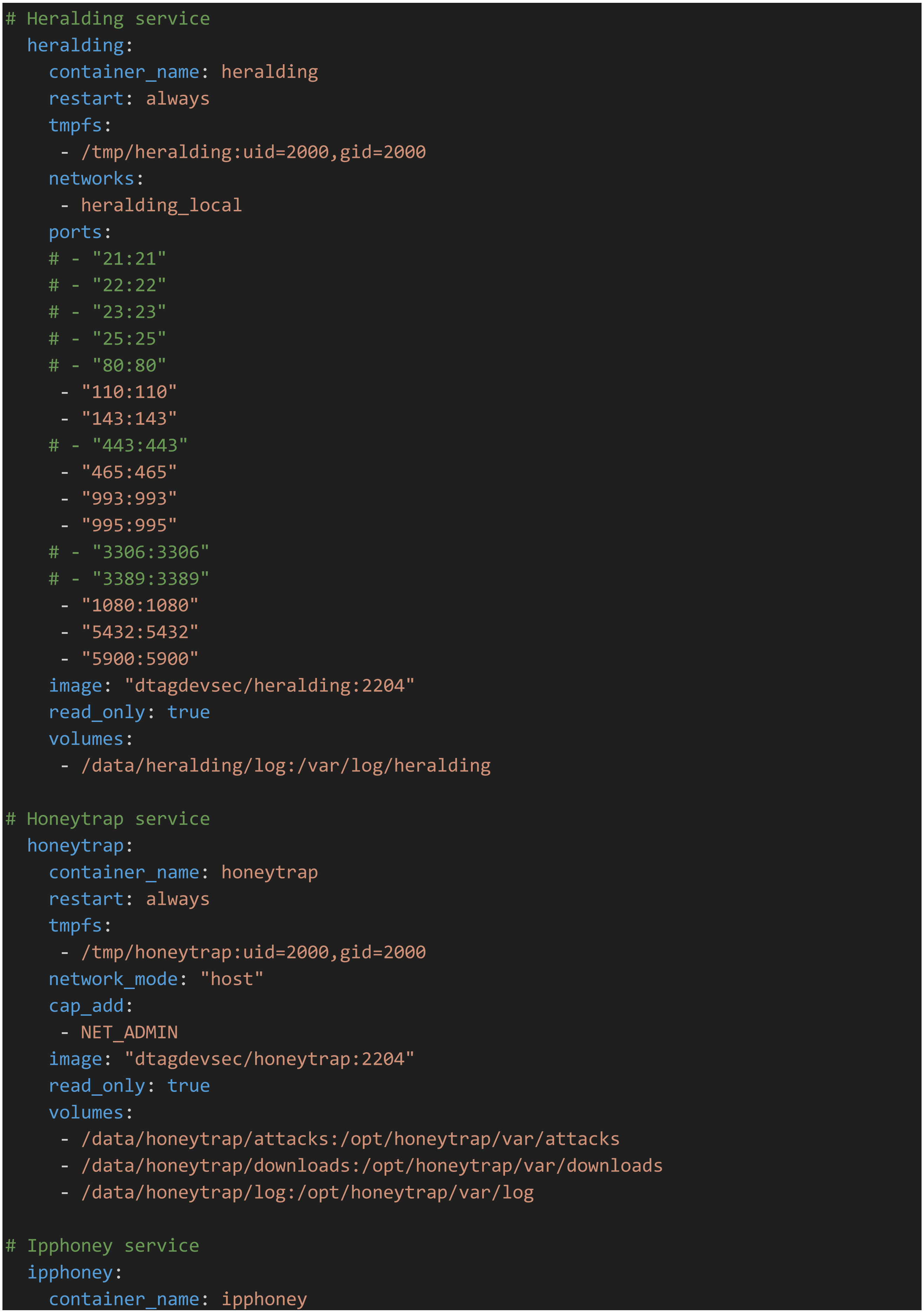
Tpot Configuration Tpot.YML (ELK connectivity with HoneyPots Container)

```
# T-Pot (Standard)
# Do not erase ports sections, these are used by /opt/tpot/bin/rules.sh to setup
iptables ACCEPT rules for NFQ (honeytrap / glutton)
version: '2.3'

networks:
  adbhoney_local:
  ciscoasa_local:
  citrixhoneypot_local:
  conpot_local_IEC104:
  conpot_local_guardian_ast:
  conpot_local_ipmi:
  conpot_local_kamstrup_382:
  cowrie_local:
  ddospot_local:
  dicompot_local:
  dionaea_local:
  elasticpot_local:
  heralding_local:
  ipphoney_local:
  mailoney_local:
  medpot_local:
  redishoneypot_local:
  tanner_local:
  ewsposter_local:
```

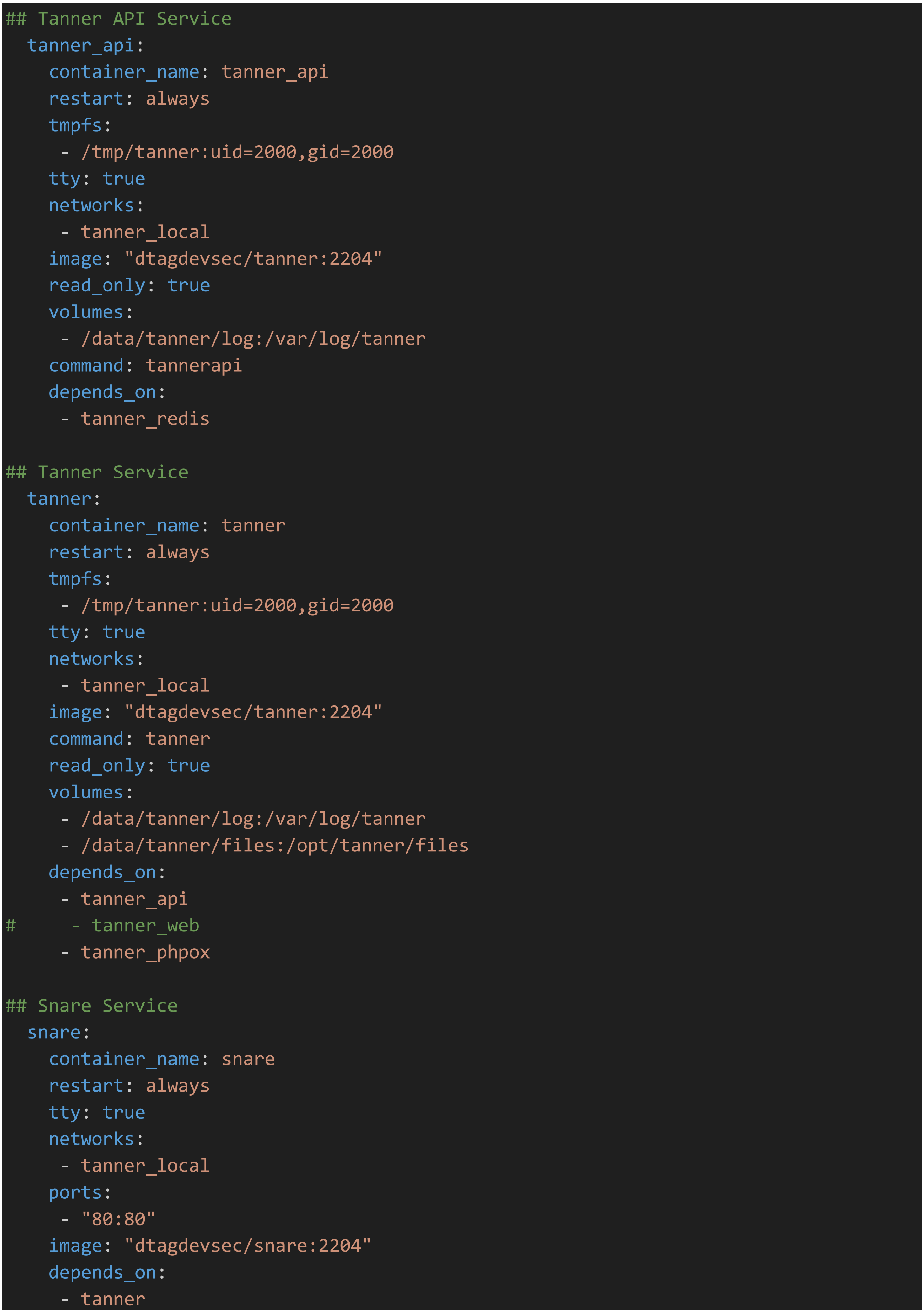
```
  sentrypeer_local:
  spiderfoot_local:

services:

##################
#### Honeypots
##################

# Adbhoney service
  adbhoney:
    container_name: adbhoney
    restart: always
    networks:
     - adbhoney_local
    ports:
     - "5555:5555"
    image: "dtagdevsec/adbhoney:2204"
    read_only: true
    volumes:
     - /data/adbhoney/log:/opt/adbhoney/log
     - /data/adbhoney/downloads:/opt/adbhoney/dl

# Ciscoasa service
  ciscoasa:
    container_name: ciscoasa
    restart: always
    tmpfs:
     - /tmp/ciscoasa:uid=2000,gid=2000
    networks:
     - ciscoasa_local
    ports:
     - "5000:5000/udp"
     - "8443:8443"
    image: "dtagdevsec/ciscoasa:2204"
    read_only: true
    volumes:
     - /data/ciscoasa/log:/var/log/ciscoasa

# CitrixHoneypot service
  citrixhoneypot:
    container_name: citrixhoneypot
    restart: always
    networks:
     - citrixhoneypot_local
    ports:
     - "443:443"
    image: "dtagdevsec/citrixhoneypot:2204"
    read_only: true
    volumes:
     - /data/citrixhoneypot/logs:/opt/citrixhoneypot/logs

# Conpot IEC104 service
  conpot_IEC104:
    container_name: conpot_iec104
    restart: always
    environment:
     - CONPOT_CONFIG=/etc/conpot/conpot.cfg
     - CONPOT_JSON_LOG=/var/log/conpot/conpot_IEC104.json
     - CONPOT_LOG=/var/log/conpot/conpot_IEC104.log
     - CONPOT_TEMPLATE=IEC104
     - CONPOT_TMP=/tmp/conpot
    tmpfs:
     - /tmp/conpot:uid=2000,gid=2000
    networks:
     - conpot_local_IEC104
    ports:
     - "161:161/udp"
     - "2404:2404"
    image: "dtagdevsec/conpot:2204"
    read_only: true
    volumes:
     - /data/conpot/log:/var/log/conpot

# Conpot guardian_ast service
  conpot_guardian_ast:
    container_name: conpot_guardian_ast
    restart: always
    environment:
     - CONPOT_CONFIG=/etc/conpot/conpot.cfg
     - CONPOT_JSON_LOG=/var/log/conpot/conpot_guardian_ast.json
     - CONPOT_LOG=/var/log/conpot/conpot_guardian_ast.log
     - CONPOT_TEMPLATE=guardian_ast
     - CONPOT_TMP=/tmp/conpot
    tmpfs:
     - /tmp/conpot:uid=2000,gid=2000
    networks:
     - conpot_local_guardian_ast
    ports:
     - "10001:10001"
    image: "dtagdevsec/conpot:2204"
    read_only: true
    volumes:
     - /data/conpot/log:/var/log/conpot

# Conpot ipmi
  conpot_ipmi:
    container_name: conpot_ipmi
    restart: always
    environment:
     - CONPOT_CONFIG=/etc/conpot/conpot.cfg
     - CONPOT_JSON_LOG=/var/log/conpot/conpot_ipmi.json
     - CONPOT_LOG=/var/log/conpot/conpot_ipmi.log
     - CONPOT_TEMPLATE=ipmi
     - CONPOT_TMP=/tmp/conpot
    tmpfs:
     - /tmp/conpot:uid=2000,gid=2000
    networks:
     - conpot_local_ipmi
    ports:
     - "623:623/udp"
    image: "dtagdevsec/conpot:2204"
    read_only: true
    volumes:
     - /data/conpot/log:/var/log/conpot

# Conpot kamstrup_382
  conpot_kamstrup_382:
    container_name: conpot_kamstrup_382
    restart: always
    environment:
     - CONPOT_CONFIG=/etc/conpot/conpot.cfg
     - CONPOT_JSON_LOG=/var/log/conpot/conpot_kamstrup_382.json
     - CONPOT_LOG=/var/log/conpot/conpot_kamstrup_382.log
     - CONPOT_TEMPLATE=kamstrup_382
     - CONPOT_TMP=/tmp/conpot
    tmpfs:
     - /tmp/conpot:uid=2000,gid=2000
    networks:
     - conpot_local_kamstrup_382
    ports:
     - "1025:1025"
     - "50100:50100"
    image: "dtagdevsec/conpot:2204"
    read_only: true
    volumes:
     - /data/conpot/log:/var/log/conpot

# Cowrie service
  cowrie:
    container_name: cowrie
    restart: always
    tmpfs:
     - /tmp/cowrie:uid=2000,gid=2000
     - /tmp/cowrie/data:uid=2000,gid=2000
    networks:
     - cowrie_local
    ports:
     - "22:22"
     - "23:23"
    image: "dtagdevsec/cowrie:2204"
    read_only: true
    volumes:
     - /data/cowrie/downloads:/home/cowrie/cowrie/dl
     - /data/cowrie/keys:/home/cowrie/cowrie/etc
     - /data/cowrie/log:/home/cowrie/cowrie/log
     - /data/cowrie/log/tty:/home/cowrie/cowrie/log/tty

# Ddospot service
  ddospot:
    container_name: ddospot
    restart: always
    networks:
     - ddospot_local
    ports:
     - "19:19/udp"
     - "53:53/udp"
     - "123:123/udp"
#     - "161:161/udp"
     - "1900:1900/udp"
    image: "dtagdevsec/ddospot:2204"
    read_only: true
    volumes:
     - /data/ddospot/log:/opt/ddospot/ddospot/logs
     - /data/ddospot/bl:/opt/ddospot/ddospot/bl
     - /data/ddospot/db:/opt/ddospot/ddospot/db

# Dicompot service
# Get the Horos Client for testing: https://horosproject.org/
# Get Dicom images (CC BY 3.0): https://www.cancerimagingarchive.net/collections/
# Put images (which must be in Dicom DCM format or it will not work!) into
/data/dicompot/images
  dicompot:
    container_name: dicompot
    restart: always
    networks:
     - dicompot_local
    ports:
     - "11112:11112"
    image: "dtagdevsec/dicompot:2204"
    read_only: true
    volumes:
     - /data/dicompot/log:/var/log/dicompot
#     - /data/dicompot/images:/opt/dicompot/images

# Dionaea service
```



```
  dionaea:
    container_name: dionaea
    stdin_open: true
    tty: true
    restart: always
    networks:
     - dionaea_local
    ports:
     - "20:20"
     - "21:21"
     - "42:42"
     - "69:69/udp"
     - "81:81"
     - "135:135"
     # - "443:443"
     - "445:445"
     - "1433:1433"
     - "1723:1723"
     - "1883:1883"
     - "3306:3306"
     # - "5060:5060"
     # - "5060:5060/udp"
     # - "5061:5061"
     - "27017:27017"
    image: "dtagdevsec/dionaea:2204"
    read_only: true
    volumes:
     - /data/dionaea/roots/ftp:/opt/dionaea/var/dionaea/roots/ftp
     - /data/dionaea/roots/tftp:/opt/dionaea/var/dionaea/roots/tftp
     - /data/dionaea/roots/www:/opt/dionaea/var/dionaea/roots/www
     - /data/dionaea/roots/upnp:/opt/dionaea/var/dionaea/roots/upnp
     - /data/dionaea:/opt/dionaea/var/dionaea
     - /data/dionaea/binaries:/opt/dionaea/var/dionaea/binaries
     - /data/dionaea/log:/opt/dionaea/var/log
     - /data/dionaea/rtp:/opt/dionaea/var/dionaea/rtp

# ElasticPot service
  elasticpot:
    container_name: elasticpot
    restart: always
    networks:
     - elasticpot_local
    ports:
     - "9200:9200"
    image: "dtagdevsec/elasticpot:2204"
    read_only: true
    volumes:
     - /data/elasticpot/log:/opt/elasticpot/log
```



```
# Heralding service
  heralding:
    container_name: heralding
    restart: always
    tmpfs:
     - /tmp/heralding:uid=2000,gid=2000
    networks:
     - heralding_local
    ports:
    # - "21:21"
    # - "22:22"
    # - "23:23"
    # - "25:25"
    # - "80:80"
     - "110:110"
     - "143:143"
    # - "443:443"
     - "465:465"
     - "993:993"
     - "995:995"
    # - "3306:3306"
    # - "3389:3389"
     - "1080:1080"
     - "5432:5432"
     - "5900:5900"
    image: "dtagdevsec/heralding:2204"
    read_only: true
    volumes:
     - /data/heralding/log:/var/log/heralding

# Honeytrap service
  honeytrap:
    container_name: honeytrap
    restart: always
    tmpfs:
     - /tmp/honeytrap:uid=2000,gid=2000
    network_mode: "host"
    cap_add:
     - NET_ADMIN
    image: "dtagdevsec/honeytrap:2204"
    read_only: true
    volumes:
     - /data/honeytrap/attacks:/opt/honeytrap/var/attacks
     - /data/honeytrap/downloads:/opt/honeytrap/var/downloads
     - /data/honeytrap/log:/opt/honeytrap/var/log

# Ipphoney service
  ipphoney:
    container_name: ipphoney
    restart: always
    networks:
     - ipphoney_local
    ports:
     - "631:631"
    image: "dtagdevsec/ipphoney:2204"
    read_only: true
    volumes:
     - /data/ipphoney/log:/opt/ipphoney/log

# Mailoney service
  mailoney:
    container_name: mailoney
    restart: always
    environment:
     - HPFEEDS_SERVER=
     - HPFEEDS_IDENT=user
     - HPFEEDS_SECRET=pass
     - HPFEEDS_PORT=20000
     - HPFEEDS_CHANNELPREFIX=prefix
    networks:
     - mailoney_local
    ports:
     - "25:25"
    image: "dtagdevsec/mailoney:2204"
    read_only: true
    volumes:
     - /data/mailoney/log:/opt/mailoney/logs

# Medpot service
  medpot:
    container_name: medpot
    restart: always
    networks:
     - medpot_local
    ports:
     - "2575:2575"
    image: "dtagdevsec/medpot:2204"
    read_only: true
    volumes:
     - /data/medpot/log/:/var/log/medpot

# Redishoneypot service
  redishoneypot:
    container_name: redishoneypot
    restart: always
    networks:
     - redishoneypot_local
    ports:
     - "6379:6379"
    image: "dtagdevsec/redishoneypot:2204"
    read_only: true
    volumes:
     - /data/redishoneypot/log:/var/log/redishoneypot

# SentryPeer service
  sentrypeer:
    container_name: sentrypeer
    restart: always
# SentryPeer offers to exchange bad actor data via DHT / P2P mode by setting the ENV to true (1)
# In some cases (i.e. internally deployed T-Pots) this might be confusing as SentryPeer will show
# the bad actors in its logs. Therefore this option is opt-in based.
#    environment:
#     - SENTRYPEER_PEER_TO_PEER=0
    networks:
     - sentrypeer_local
    ports:
#     - "4222:4222/udp"
     - "5060:5060/udp"
#     - "127.0.0.1:8082:8082"
    image: "dtagdevsec/sentrypeer:2204"
    read_only: true
    volumes:
     - /data/sentrypeer/log:/var/log/sentrypeer

#### Snare / Tanner
## Tanner Redis Service
  tanner_redis:
    container_name: tanner_redis
    restart: always
    tty: true
    networks:
     - tanner_local
    image: "dtagdevsec/redis:2204"
    read_only: true

## PHP Sandbox service
  tanner_phpox:
    container_name: tanner_phpox
    restart: always
    tty: true
    networks:
     - tanner_local
    image: "dtagdevsec/phpox:2204"
    read_only: true
```

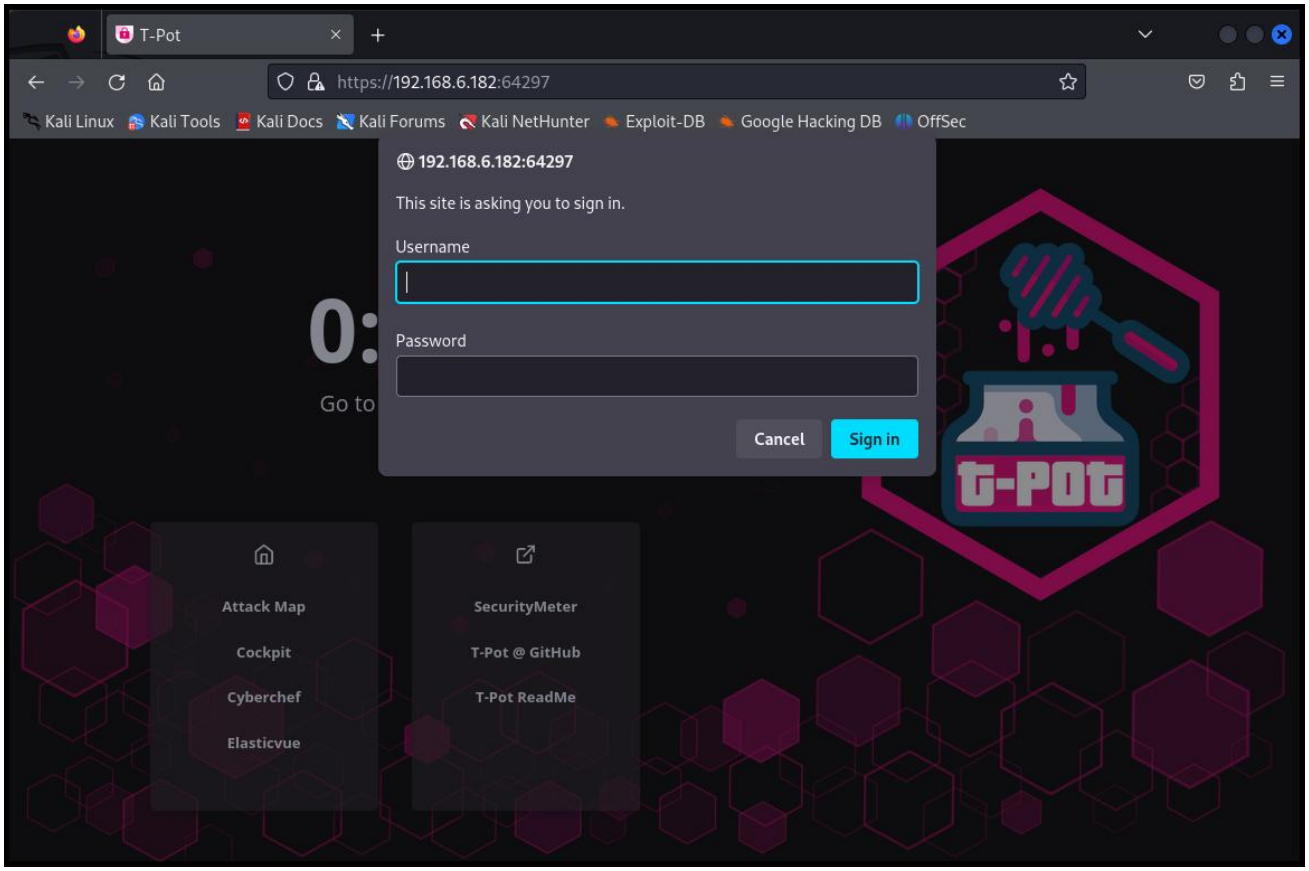


```
## Tanner API Service
  tanner_api:
    container_name: tanner_api
    restart: always
    tmpfs:
     - /tmp/tanner:uid=2000,gid=2000
    tty: true
    networks:
     - tanner_local
    image: "dtagdevsec/tanner:2204"
    read_only: true
    volumes:
     - /data/tanner/log:/var/log/tanner
    command: tannerapi
    depends_on:
     - tanner_redis

## Tanner Service
  tanner:
    container_name: tanner
    restart: always
    tmpfs:
     - /tmp/tanner:uid=2000,gid=2000
    tty: true
    networks:
     - tanner_local
    image: "dtagdevsec/tanner:2204"
    command: tanner
    read_only: true
    volumes:
     - /data/tanner/log:/var/log/tanner
     - /data/tanner/files:/opt/tanner/files
    depends_on:
     - tanner_api
#      - tanner_web
     - tanner_phpox

## Snare Service
  snare:
    container_name: snare
    restart: always
    tty: true
    networks:
     - tanner_local
    ports:
     - "80:80"
    image: "dtagdevsec/snare:2204"
    depends_on:
     - tanner
```

```
##################
#### NSM
##################

# Fatt service
  fatt:
    container_name: fatt
    restart: always
    network_mode: "host"
    cap_add:
     - NET_ADMIN
     - SYS_NICE
     - NET_RAW
    image: "dtagdevsec/fatt:2204"
    volumes:
     - /data/fatt/log:/opt/fatt/log

# P0f service
  p0f:
    container_name: p0f
    restart: always
    network_mode: "host"
    image: "dtagdevsec/p0f:2204"
    read_only: true
    volumes:
     - /data/p0f/log:/var/log/p0f

# Suricata service
  suricata:
    container_name: suricata
    restart: always
    environment:
    # For ET Pro ruleset replace "OPEN" with your OINKCODE
     - OINKCODE=OPEN
    # Loading externel Rules from URL
    # -
FROMURL="https://username:password@yoururl.com|https://username:password@otherurl.co
m"
    network_mode: "host"
    cap_add:
     - NET_ADMIN
     - SYS_NICE
     - NET_RAW
    image: "dtagdevsec/suricata:2204"
    volumes:
     - /data/suricata/log:/var/log/suricata
```

```
##################
#### Tools
##################

#### ELK
## Elasticsearch service
  elasticsearch:
    container_name: elasticsearch
    restart: always
    environment:
     - bootstrap.memory_lock=true
     - ES_JAVA_OPTS=-Xms2048m -Xmx2048m
     - ES_TMPDIR=/tmp
    cap_add:
     - IPC_LOCK
    ulimits:
      memlock:
        soft: -1
        hard: -1
      nofile:
        soft: 65536
        hard: 65536
    mem_limit: 4g
    ports:
     - "127.0.0.1:64298:9200"
    image: "dtagdevsec/elasticsearch:2204"
    volumes:
     - /data:/data

## Kibana service
  kibana:
    container_name: kibana
    restart: always
    depends_on:
      elasticsearch:
        condition: service_healthy
    mem_limit: 1g
    ports:
     - "127.0.0.1:64296:5601"
    image: "dtagdevsec/kibana:2204"

## Logstash service
  logstash:
    container_name: logstash
    restart: always
    environment:
     - LS_JAVA_OPTS=-Xms1024m -Xmx1024m
    depends_on:
      elasticsearch:
        condition: service_healthy
    env_file:
     - /opt/tpot/etc/compose/elk_environment
    mem_limit: 2g
    image: "dtagdevsec/logstash:2204"
    volumes:
     - /data:/data

## Map Redis Service
  map_redis:
    container_name: map_redis
    restart: always
    stop_signal: SIGKILL
    tty: true
    image: "dtagdevsec/redis:2204"
    read_only: true

## Map Web Service
  map_web:
    container_name: map_web
    restart: always
    environment:
     - MAP_COMMAND=AttackMapServer.py
    env_file:
     - /opt/tpot/etc/compose/elk_environment
    stop_signal: SIGKILL
    tty: true
    ports:
     - "127.0.0.1:64299:64299"
    image: "dtagdevsec/map:2204"

## Map Data Service
  map_data:
    container_name: map_data
    restart: always
    depends_on:
      elasticsearch:
        condition: service_healthy
    environment:
     - MAP_COMMAND=DataServer_v2.py
    env_file:
     - /opt/tpot/etc/compose/elk_environment
    stop_signal: SIGKILL
    tty: true
    image: "dtagdevsec/map:2204"
#### /ELK

# Ewsposter service
  ewsposter:
    container_name: ewsposter
    restart: always
    networks:
     - ewsposter_local
    environment:
     - EWS_HPFEEDS_ENABLE=false
     - EWS_HPFEEDS_HOST=host
     - EWS_HPFEEDS_PORT=port
     - EWS_HPFEEDS_CHANNELS=channels
     - EWS_HPFEEDS_IDENT=user
     - EWS_HPFEEDS_SECRET=secret
     - EWS_HPFEEDS_TLSCERT=false
     - EWS_HPFEEDS_FORMAT=json
    env_file:
     - /opt/tpot/etc/compose/elk_environment
    image: "dtagdevsec/ewsposter:2204"
    volumes:
     - /data:/data
     - /data/ews/conf/ews.ip:/opt/ewsposter/ews.ip

# Nginx service
  nginx:
    container_name: nginx
    restart: always
    tmpfs:
     - /var/tmp/nginx/client_body
     - /var/tmp/nginx/proxy
     - /var/tmp/nginx/fastcgi
     - /var/tmp/nginx/uwsgi
     - /var/tmp/nginx/scgi
     - /run
     - /var/lib/nginx/tmp:uid=100,gid=82
    network_mode: "host"
      #    ports:
      #     - "64297:64297"
      #     - "127.0.0.1:64304:64304"
    image: "dtagdevsec/nginx:2204"
    read_only: true
    volumes:
     - /data/nginx/cert/:/etc/nginx/cert/:ro
     - /data/nginx/conf/nginxpasswd:/etc/nginx/nginxpasswd:ro
     - /data/nginx/log/:/var/log/nginx/

# Spiderfoot service
  spiderfoot:
    container_name: spiderfoot
    restart: always
    networks:
     - spiderfoot_local
    ports:
     - "127.0.0.1:64303:8080"
    image: "dtagdevsec/spiderfoot:2204"
    volumes:
     - /data/spiderfoot:/home/spiderfoot/.spiderfoot
```

Dashboard of T-Pot



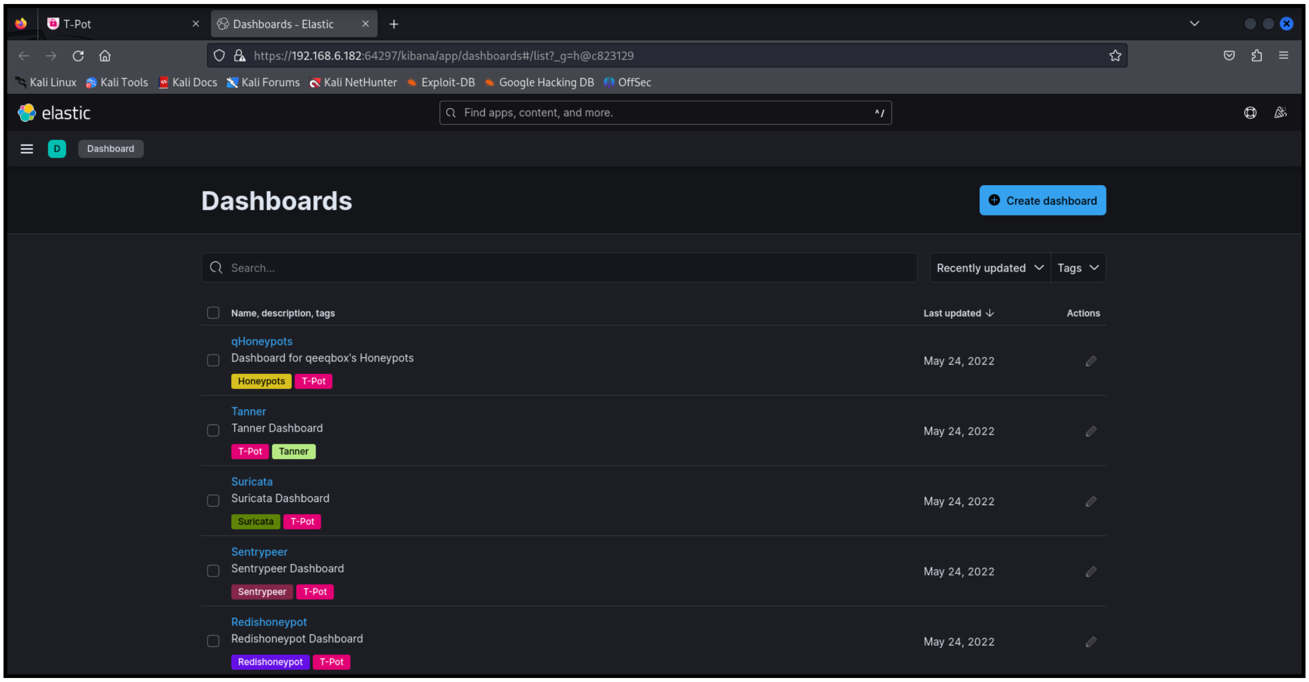
https://192.168.6.182:64297

192.168.6.182:64297

This site is asking you to sign in.

Username

Password



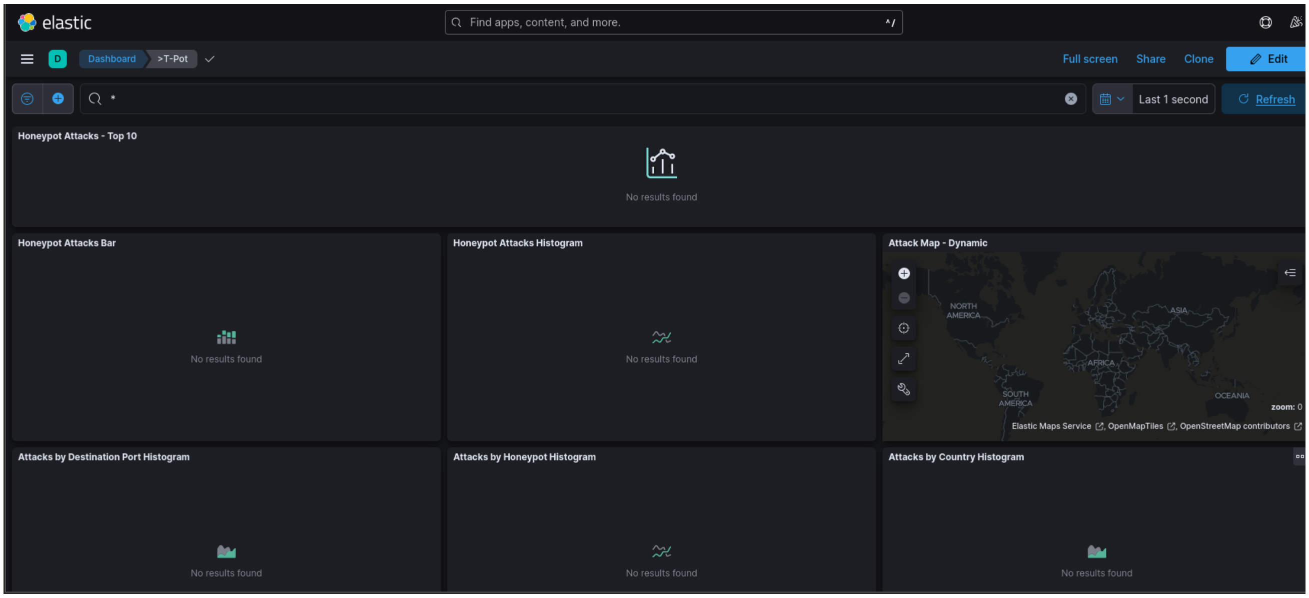
Dashboards

Create dashboard

Search...

Recently updated | Tags

Name, description, tags	Last updated	Actions
qHoneypots Dashboard for qeeqbox's Honeypots Honeypots T-Pot	May 24, 2022	
Tanner Tanner Dashboard T-Pot Tanner	May 24, 2022	
Suricata Suricata Dashboard Suricata T-Pot	May 24, 2022	
Sentrypeer Sentrypeer Dashboard Sentrypeer T-Pot	May 24, 2022	
Redishoneypot Redishoneypot Dashboard Redishoneypot T-Pot	May 24, 2022	



Honeypot Attacks - Top 10

No results found

Honeypot Attacks Bar

No results found

Honeypot Attacks Histogram

No results found

Attack Map - Dynamic

Attacks by Destination Port Histogram

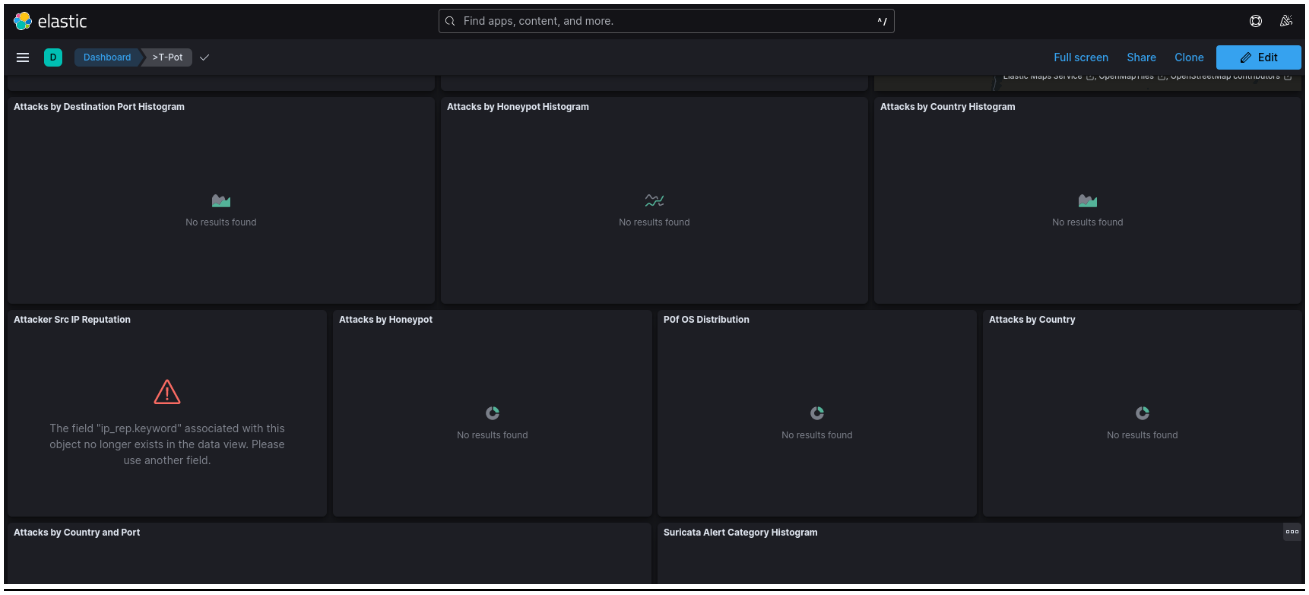
No results found

Attacks by Honeypot Histogram

No results found

Attacks by Country Histogram

No results found


elastic
Find apps, content, and more.
Dashboard
>T-Pot
Full screen
Share
Clone
Edit
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

Attacks by Destination Port Histogram

No results found

Attacks by Honeypot Histogram

No results found

Attacks by Country Histogram

No results found

Attacker Src IP Reputation

The field "ip_rep.keyword" associated with this object no longer exists in the data view. Please use another field.

Attacks by Honeypot

No results found

P0f OS Distribution

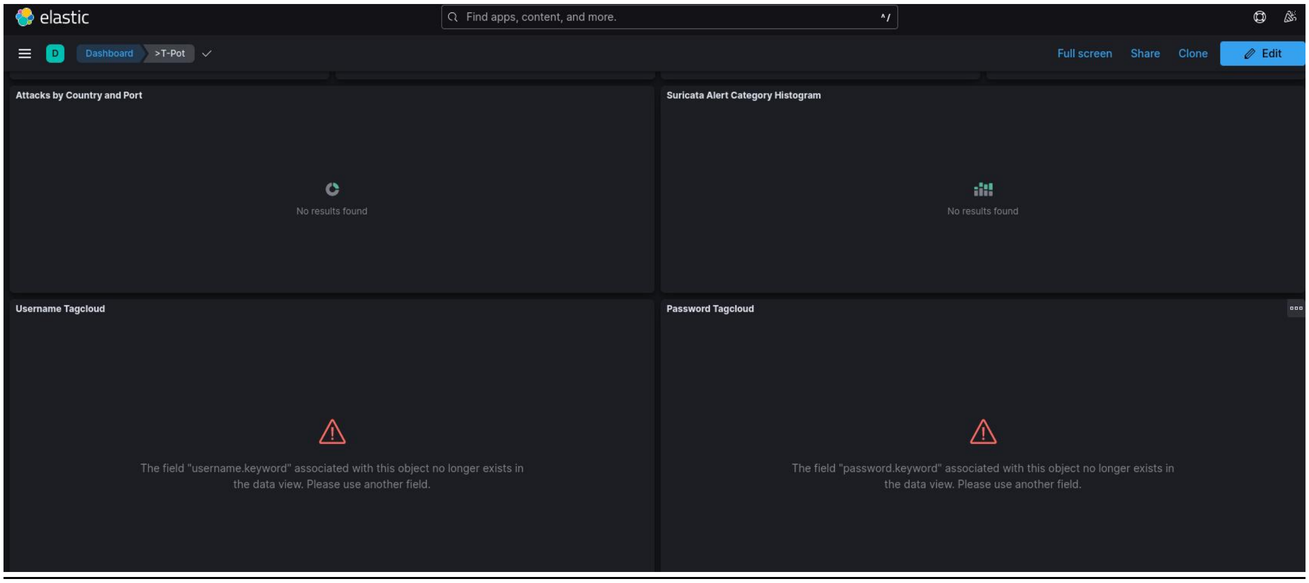
No results found

Attacks by Country

No results found

Attacks by Country and Port

Suricata Alert Category Histogram



Attacks by Country and Port

No results found

Suricata Alert Category Histogram

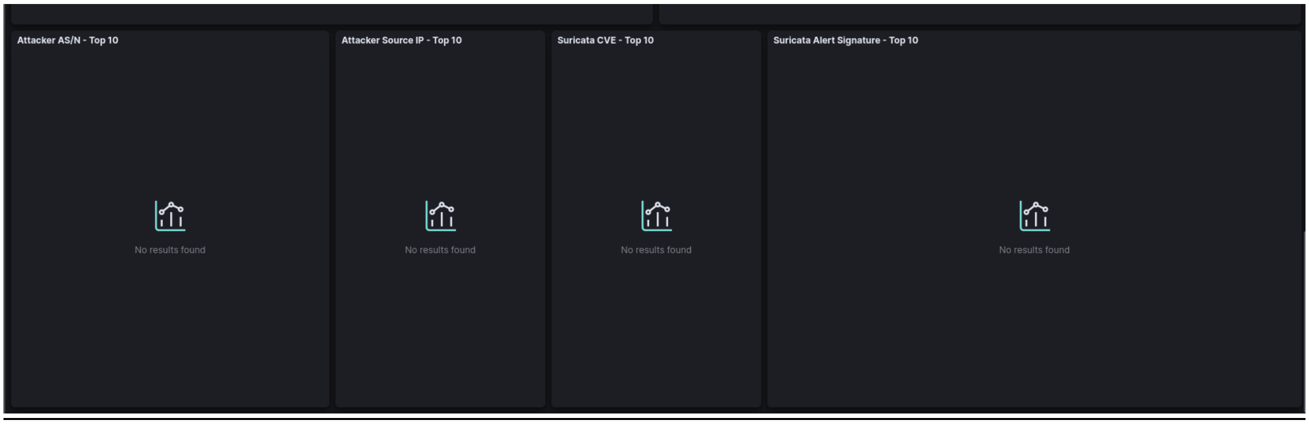
No results found

Username Tagcloud

The field "username.keyword" associated with this object no longer exists in the data view. Please use another field.

Password Tagcloud

The field "password.keyword" associated with this object no longer exists in the data view. Please use another field.



Attacker AS/N - Top 10

No results found

Attacker Source IP - Top 10

No results found

Suricata CVE - Top 10

No results found

Suricata Alert Signature - Top 10

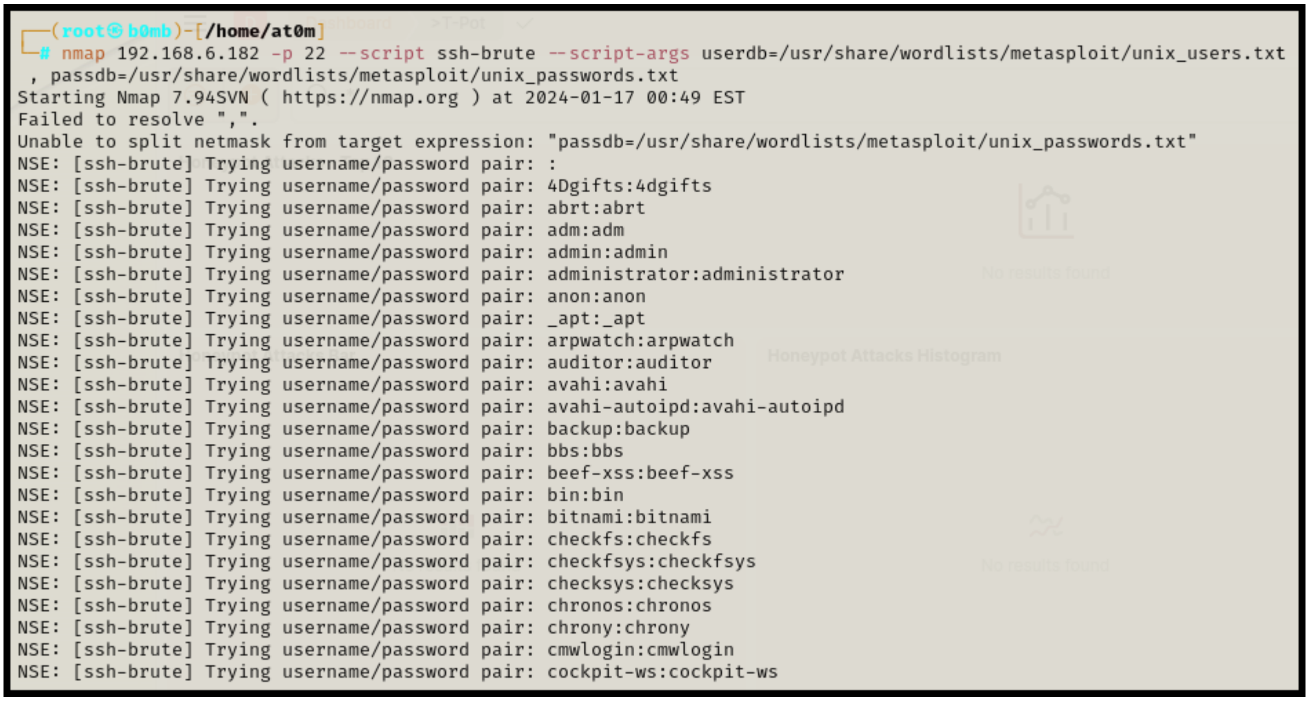
No results found

Attacking the Host: -

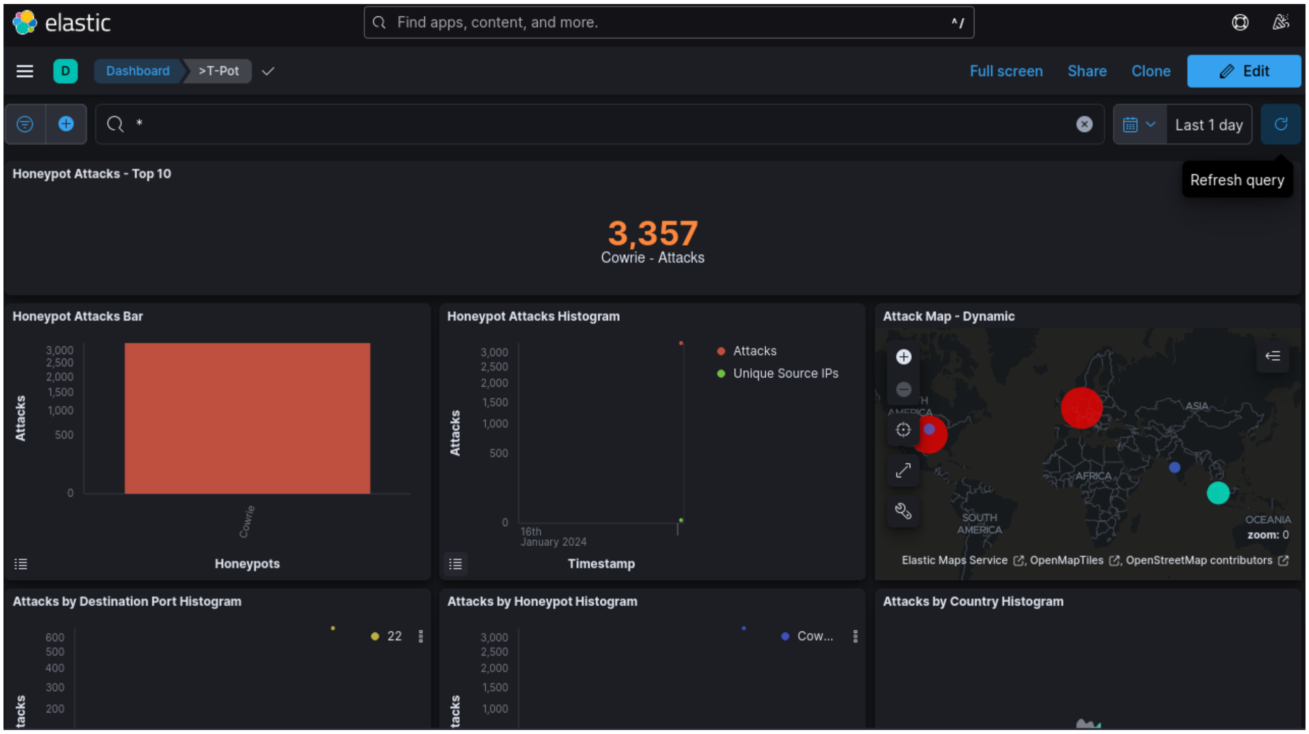
SSH BRUTE FORCE ATTACK:-

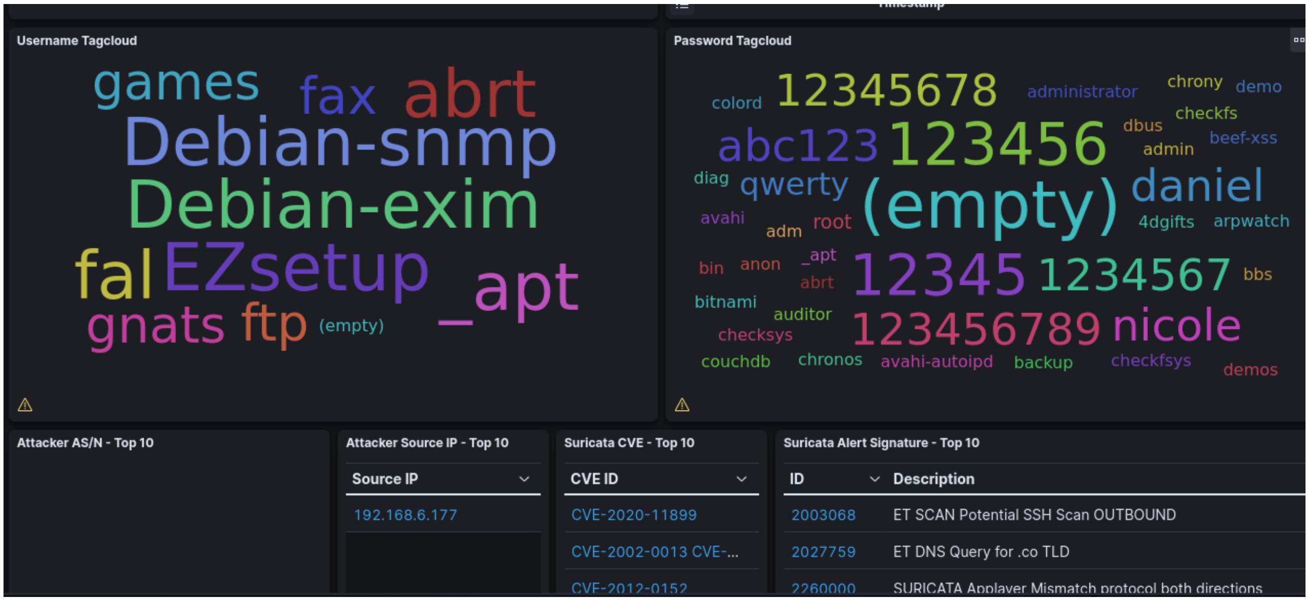
```
nmap <IPAddress> -p 22 --script ssh-brute --script-args
```

userdb=/usr/share/wordlists/metasploit/unix_users.txt , passdb=/usr/share/wordlists/metasploit/unix_passwords.txt



```
┌──(root㉿b0mb)-[/home/at0m]
└─# nmap 192.168.6.182 -p 22 --script ssh-brute --script-args userdb=/usr/share/wordlists/metasploit/unix_users.txt
 , passdb=/usr/share/wordlists/metasploit/unix_passwords.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 00:49 EST
Failed to resolve ",".
Unable to split netmask from target expression: "passdb=/usr/share/wordlists/metasploit/unix_passwords.txt"
NSE: [ssh-brute] Trying username/password pair: :
NSE: [ssh-brute] Trying username/password pair: 4Dgifts:4dgifts
NSE: [ssh-brute] Trying username/password pair: abrt:abrt
NSE: [ssh-brute] Trying username/password pair: adm:adm
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: anon:anon
NSE: [ssh-brute] Trying username/password pair: _apt:_apt
NSE: [ssh-brute] Trying username/password pair: arpwatch:arpwatch
NSE: [ssh-brute] Trying username/password pair: auditor:auditor
NSE: [ssh-brute] Trying username/password pair: avahi:avahi
NSE: [ssh-brute] Trying username/password pair: avahi-autoipd:avahi-autoipd
NSE: [ssh-brute] Trying username/password pair: backup:backup
NSE: [ssh-brute] Trying username/password pair: bbs:bbs
NSE: [ssh-brute] Trying username/password pair: beef-xss:beef-xss
NSE: [ssh-brute] Trying username/password pair: bin:bin
NSE: [ssh-brute] Trying username/password pair: bitnami:bitnami
NSE: [ssh-brute] Trying username/password pair: checkfs:checkfs
NSE: [ssh-brute] Trying username/password pair: checkfsys:checkfsys
NSE: [ssh-brute] Trying username/password pair: checksys:checksys
NSE: [ssh-brute] Trying username/password pair: chronos:chronos
NSE: [ssh-brute] Trying username/password pair: chrony:chrony
NSE: [ssh-brute] Trying username/password pair: cmwlogin:cmwlogin
NSE: [ssh-brute] Trying username/password pair: cockpit-ws:cockpit-ws
```





Attacker AS/N - Top 10

Attacker Source IP - Top 10

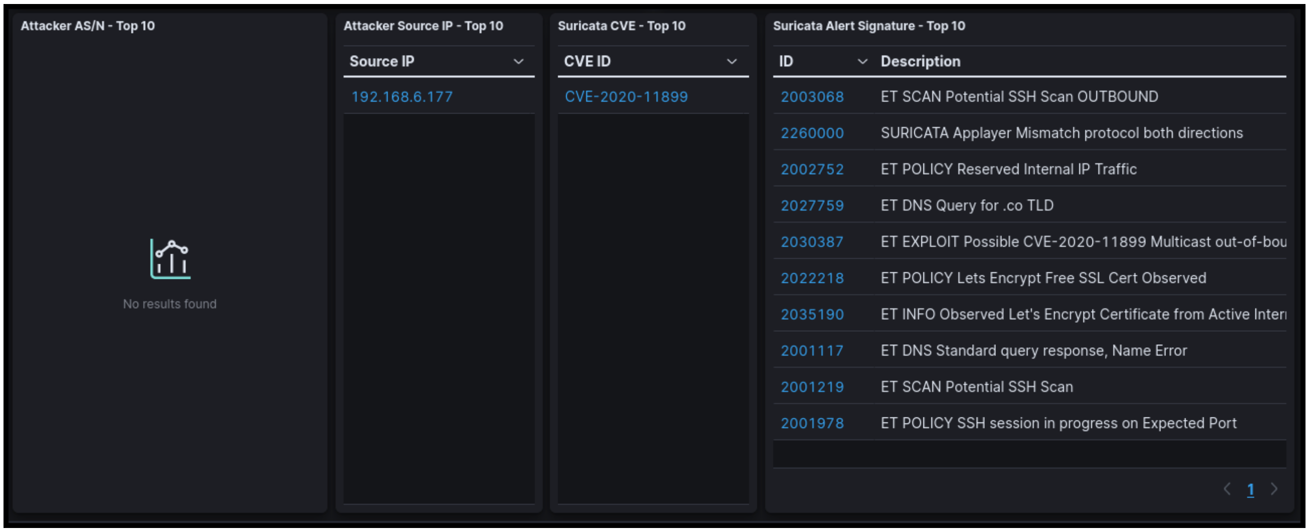
Source IP
192.168.6.177

Suricata CVE - Top 10

CVE ID
CVE-2020-11899
CVE-2002-0013 CVE-...
CVE-2012-0152

Suricata Alert Signature - Top 10

ID	Description
2003068	ET SCAN Potential SSH Scan OUTBOUND
2027759	ET DNS Query for .co TLD
2260000	SURICATA Applayer Mismatch protocol both directions



Attacker AS/N - Top 10

No results found

Attacker Source IP - Top 10

Source IP
192.168.6.177

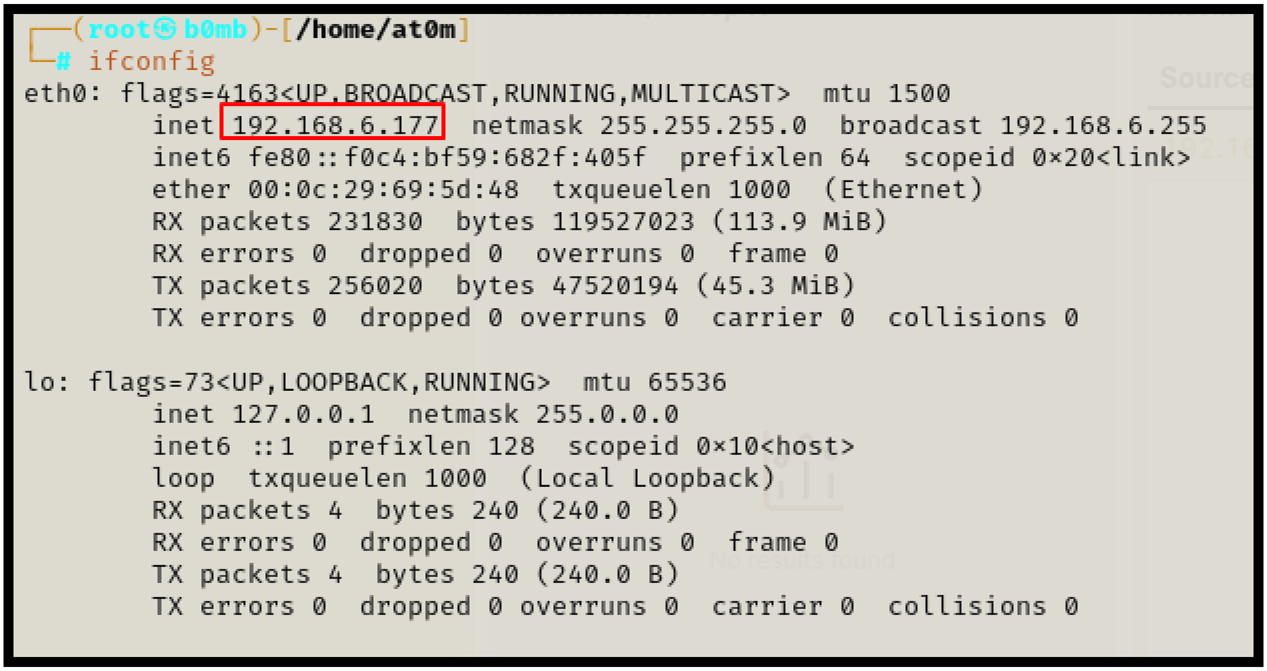
Suricata CVE - Top 10

CVE ID
CVE-2020-11899

Suricata Alert Signature - Top 10

ID	Description
2003068	ET SCAN Potential SSH Scan OUTBOUND
2260000	SURICATA Applayer Mismatch protocol both directions
2002752	ET POLICY Reserved Internal IP Traffic
2027759	ET DNS Query for .co TLD
2030387	ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bou
2022218	ET POLICY Lets Encrypt Free SSL Cert Observed
2035190	ET INFO Observed Let's Encrypt Certificate from Active Interi
2001117	ET DNS Standard query response, Name Error
2001219	ET SCAN Potential SSH Scan
2001978	ET POLICY SSH session in progress on Expected Port

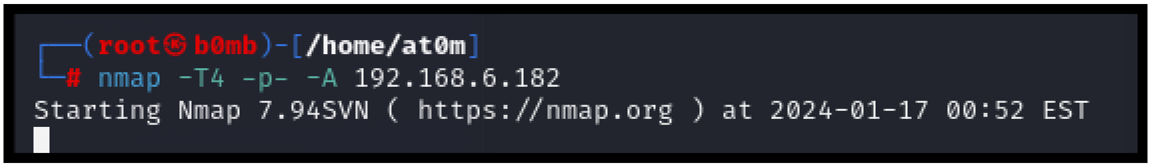
Checking the IP address of the Attacker PC



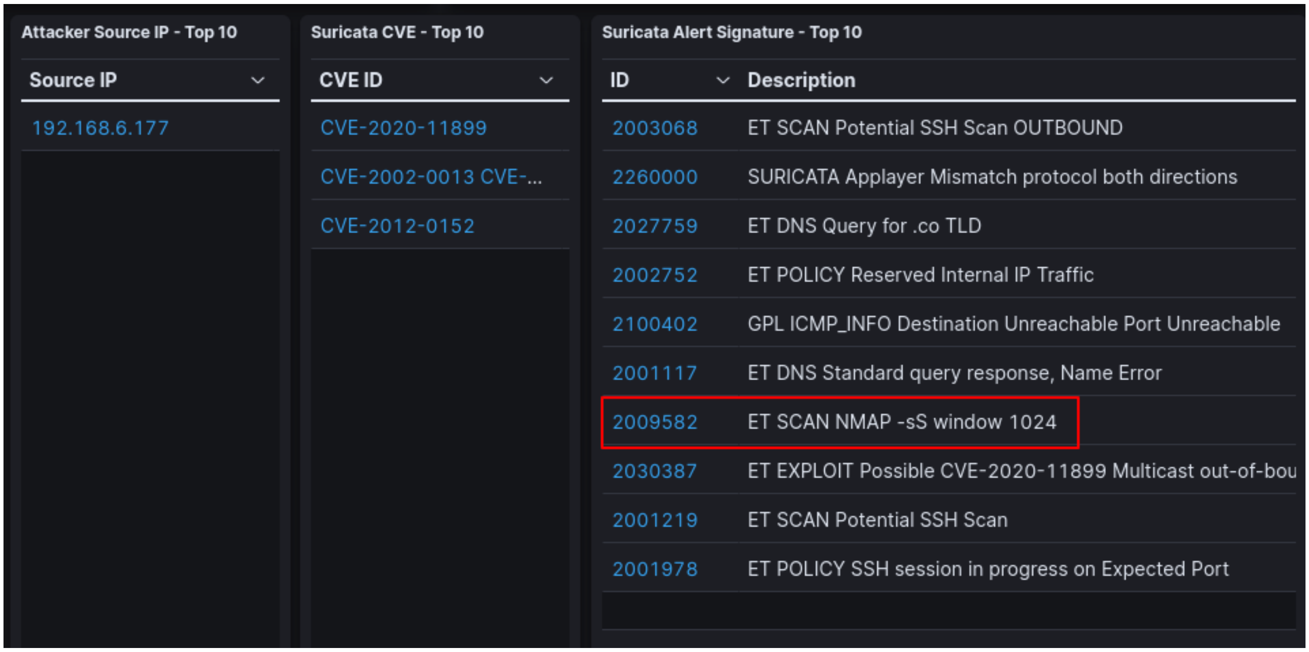
```
┌──(root㉿b0mb)-[/home/at0m]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.6.177  netmask 255.255.255.0  broadcast 192.168.6.255
        inet6 fe80::f0c4:bf59:682f:405f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:69:5d:48  txqueuelen 1000  (Ethernet)
        RX packets 231830  bytes 119527023 (113.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 256020  bytes 47520194 (45.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Running a Port Scan

nmap -T4 -p- -A 192.168.6.182



```
┌──(root㉿b0mb)-[/home/at0m]
└─# nmap -T4 -p- -A 192.168.6.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 00:52 EST
```



Attacker Source IP - Top 10

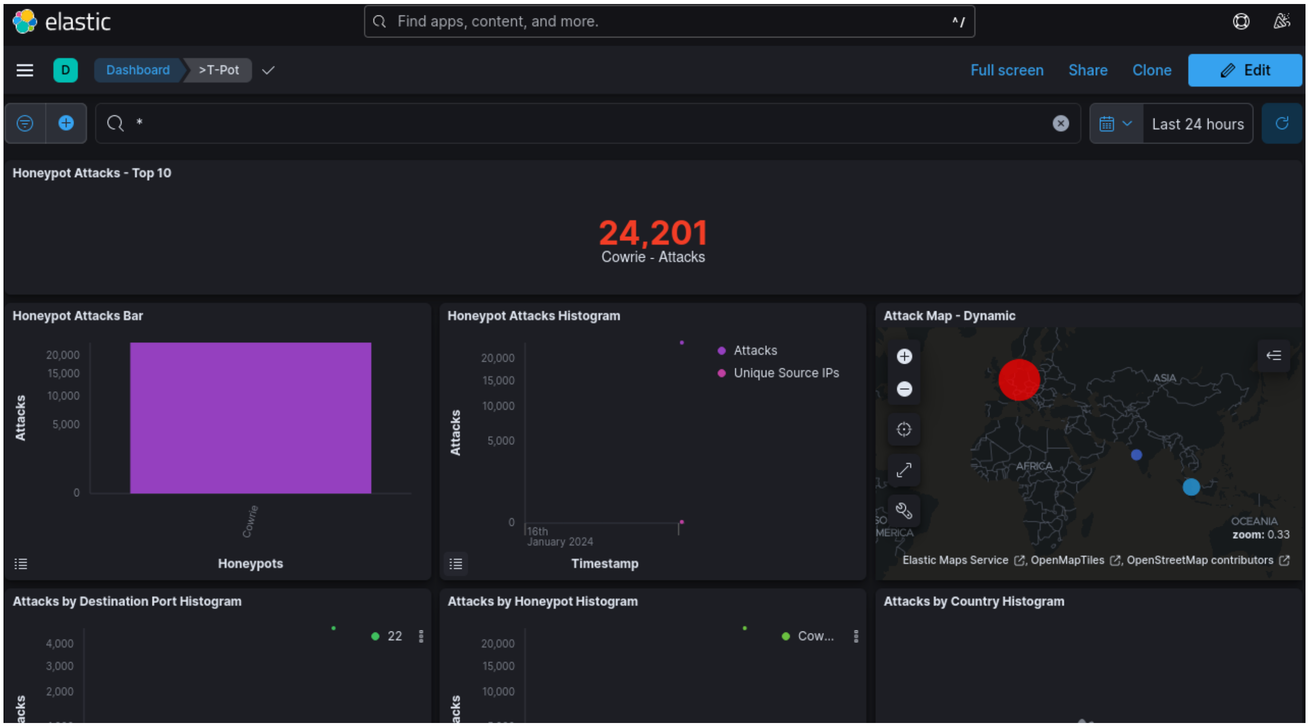
Source IP
192.168.6.177

Suricata CVE - Top 10

CVE ID
CVE-2020-11899
CVE-2002-0013 CVE-...
CVE-2012-0152

Suricata Alert Signature - Top 10

ID	Description
2003068	ET SCAN Potential SSH Scan OUTBOUND
2260000	SURICATA Applayer Mismatch protocol both directions
2027759	ET DNS Query for .co TLD
2002752	ET POLICY Reserved Internal IP Traffic
2100402	GPL ICMP_INFO Destination Unreachable Port Unreachable
2001117	ET DNS Standard query response, Name Error
2009582	ET SCAN NMAP -sS window 1024
2030387	ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bou
2001219	ET SCAN Potential SSH Scan
2001978	ET POLICY SSH session in progress on Expected Port



elastic
Find apps, content, and more.
D
Dashboard
>T-Pot
Full screen
Share
Clone
Edit
Last 24 hours
Honeypot Attacks - Top 10
24,201
Cowrie - Attacks
Honeypot Attacks Bar
20,000
15,000
10,000
5,000
0
Attacks
Cowrie
Honeypots
Honeypot Attacks Histogram
Attacks
Unique Source IPs
20,000
15,000
10,000
5,000
0
16th
January 2024
Timestamp
Attack Map - Dynamic
ASIA
AFRICA
OCEANIA
zoom: 0.33
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
Attacks by Destination Port Histogram
22
4,000
3,000
2,000
Attacks by Honeypot Histogram
Cow...
20,000
15,000
10,000
Attacks by Country Histogram