

THREAT HUNTING WORKSHOP: HUNTING FOR EXFILTRATION

V1.2



Disclaimer of Warranty

COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

Technical Assistance

Please note that because of the wide variation in individual systems and environments, **Cyborg Security is unable to provide additional technical assistance** for the purposes of configuring, using, or repairing the provided software beyond what is included in this guide.

Participants can seek assistance in the following locations:

Cyborg Security's Knowledge Base:

<https://kb.cyborgsecurity.com/knowledge>

Cyborg Security's Discord Threat Hunting Community:

<https://discord.gg/DR4mcW4zBr>

Participants are recommended to have a moderate technical background to follow along.



Minimum System Requirements

OS: Windows/OS X/Linux

Memory: 8 GB RAM

CPU: 4 cores

Free Space: 50 GB

Recommended Browser(s): Google Chrome / Microsoft Edge



Virtualbox Configuration

The following steps are centered around VirtualBox on the Windows operating system as the virtualization software for the Threat Hunting Workshop. Other virtualization technologies and operating systems can be utilized, adjusting the VirtualBox steps for the OS and software of your choosing.

Install VirtualBox:

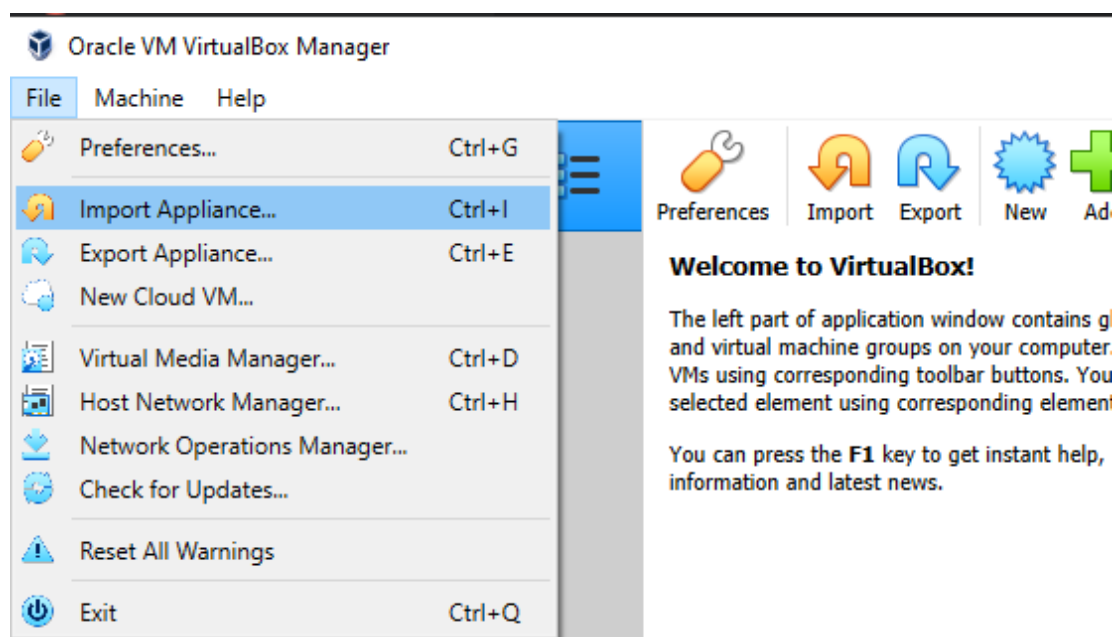
- Use the following link and instructions to install VirtualBox on the chosen OS:
 - <https://www.virtualbox.org/wiki/Downloads>

Download the Workshop virtual machine file (OVA)

- Use the following link to download the Cyborg Workshop OVA
 - <https://huntwithcyb.org/3LKAWMb>

Import the Workshop OVA

- In VirtualBox go to 'File' ⇒ 'Import Appliance' and select the downloaded OVA.





- Select OVA file location and press 'Next'
- **Optional Step:**
 - In the 'Appliance Settings' section, reconfigure the CPU or RAM depending on your local environment. The default values are the suggested resources for the workshop environment.
- Press 'Import' once the configuration options are approved.

←

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	CyborgSecurity-Workshop
Guest OS Type	Ubuntu (64-bit)
CPU	2
RAM	4096 MB
Sound Card	<input checked="" type="checkbox"/> ICH AC97
Network Adapter	<input checked="" type="checkbox"/> Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (SATA)	AHCI
Storage Controller (SCSI)	LsiLogic
Virtual Disk Image	CyborgSecurity-Workshop-disk001.vmdk
Base Folder	C:\Users\CyborgMike\VirtualBox VMs
Primary Group	/

Machine Base Folder:

MAC Address Policy:

Additional Options: ☒ Import hard drives as VDI

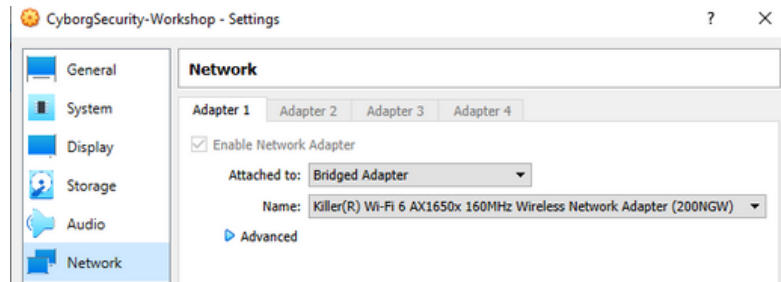
Appliance is not signed



Configure the Workshop Virtual Machine's Networking

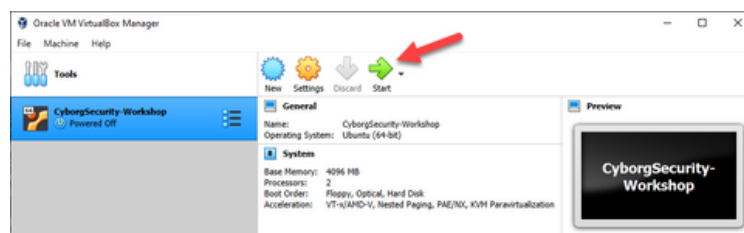
- Go to 'Machine' ⇒ 'Settings' and select the Network Tab.
- Change the 'Attached to:' setting to select the 'Bridged Adapter'.
- Press 'OK' once complete

*For MacOS Users, If you are having trouble connecting to the 'Bridged Adapter' refer to page 10



Start and login the Workshop Virtual Machine

- Press the 'Start' button in the VirtualBox Manager to turn on the Workshop virtual machine.



- Once the virtual machine as finished booting up, login using the following credentials:

Username: workshop

Password: Cyb0rgW0rksh0p!

File Locations and Services

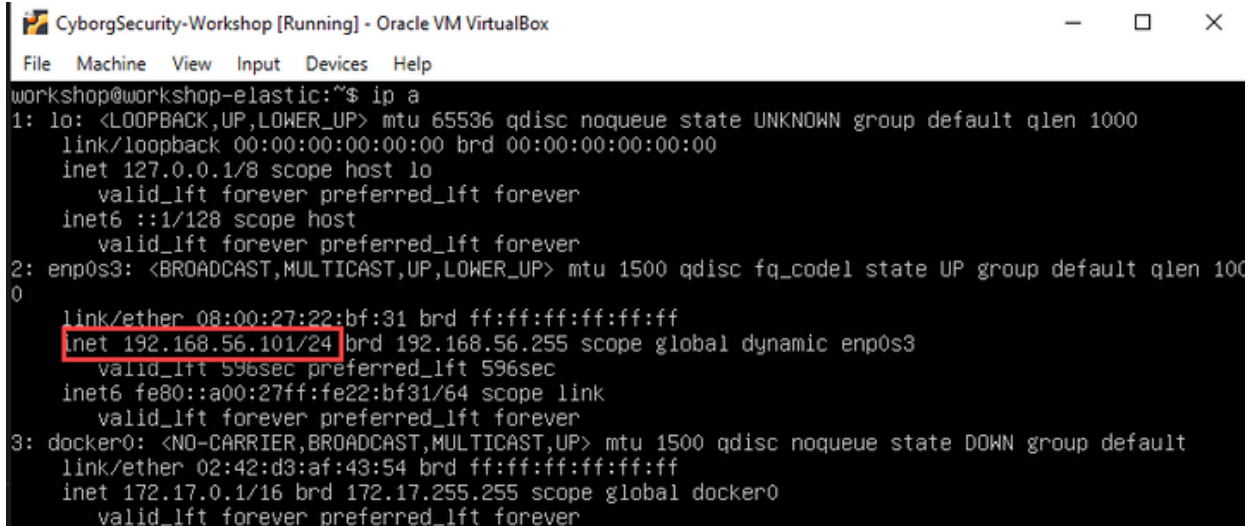
- Elasticsearch and Kibana are managed by Docker and Docker-Compose files found in the following location:
 - /home/workshop/workshop
- To check the Elasticsearch and Kibana services use the following steps:
 - `cd /home/workshop/workshop`
 - `sudo docker-compose ps`

```
workshop@workshop-elastic:~/workshop$ sudo docker-compose ps
[sudo] password for workshop:
-----
Name                                Command                                State                                Ports
-----
workshop_elasticsearch_1            /bin/tini -- /usr/local/bi           Up (healthy) • 0.0.0.0:9200->9200/tcp,:::9
...                                  ...                                   ...                                200->9200/tcp, 9300/tcp
workshop_kibana_1                   /bin/tini -- /usr/local/bi           Up (healthy)  0.0.0.0:5601->5601/tcp,:::5
...                                  ...                                   ...                                601->5601/tcp
```

- Both services should be in the 'UP' state upon starting or rebooting the virtual machine.
- Please disregard the "unhealthy" message for Kibana. You should still be able to navigate to the Kibana URI as long as the 'docker-compose ps' command shows 'UP'

Confirm IP Address of Virtual Machine

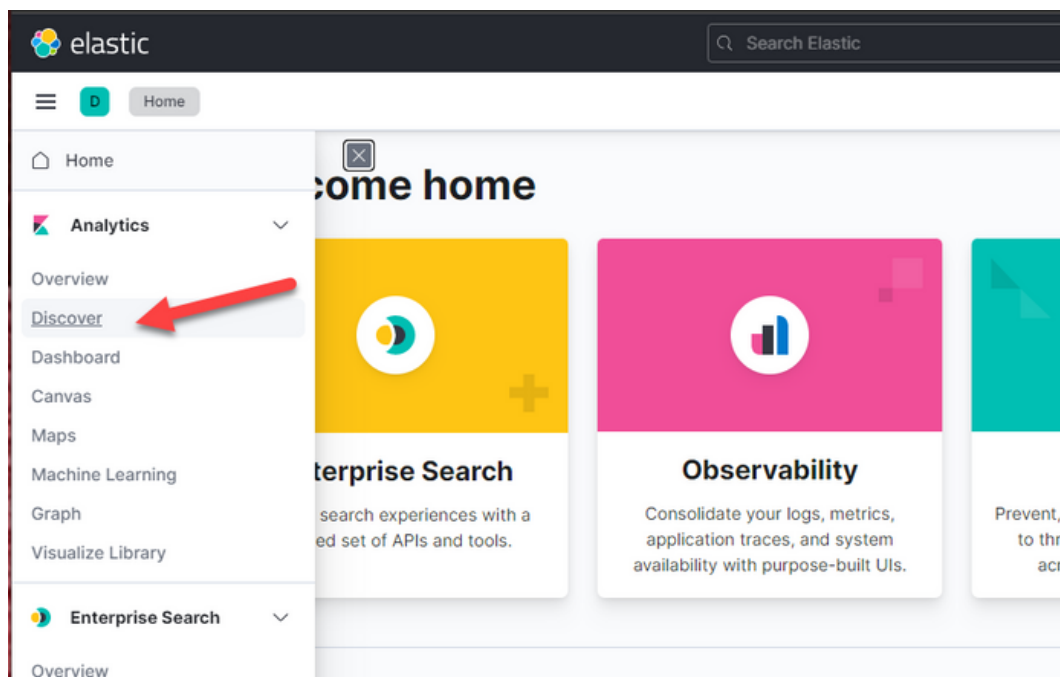
- Run the following command to get the IP Address of the virtual machine assigned by DHCP:
 - `ip a`



```
CyborgSecurity-Workshop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
workshop@workshop-elastic:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:bf:31 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic enp0s3
        valid_lft 596sec preferred_lft 596sec
    inet6 fe80::a00:27ff:fe22:bf31/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:d3:af:43:54 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

Access Kibana

- Go to the following URL and use the credentials below to access Kibana
 - `http://<IP ADDRESS>:5601`
 - Username: elastic
 - Password: Cyb0rgW0rksh0p!
- Once authenticated, open the side drawer and click on the 'Discover' option





Unzip Workshop Logs

- Use the following command to untar the Workshop logs already supplied in the OVA.
 - `cd /home/workshop`
 - `wget https://cyborg-pub.s3.us-east-2.amazonaws.com/Workshop/HuntingForExfil.tar.gz`
 - `tar zxvf HuntingForExfil.tar.gz`
- This process will create a file called
 - `'HuntingForExfil.ndjson'`
 - in the `/home/workshop/` directory

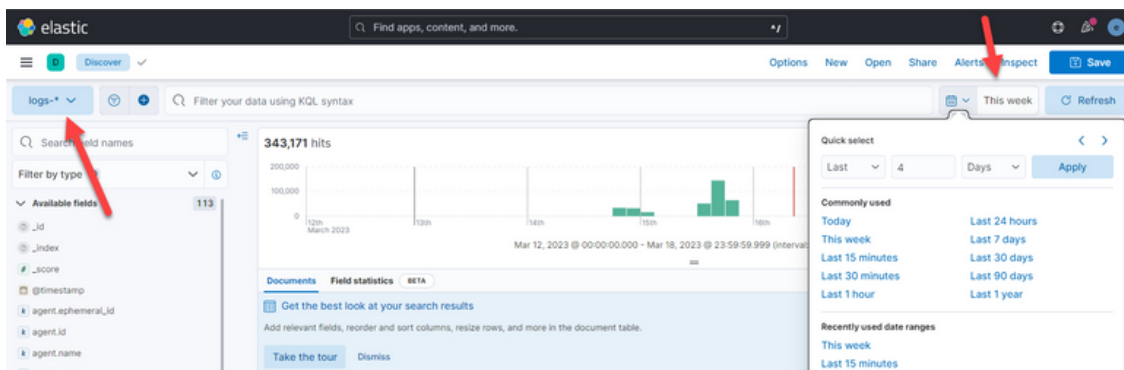
Start Workshop Log Ingestion Process

- Run the following commands to start the Workshop ingestion process by indexing the NDJSON file into the running ElasticSearch instance.
 - `cd /home/workshop/`
 - `python3 ingest_logs.py`
`/home/workshop/HuntingForExfil.ndjson`
- The script will start to ingest logs into Elastic. As the logs are ingested, the script will print to screen the current status and count of logs ingested.

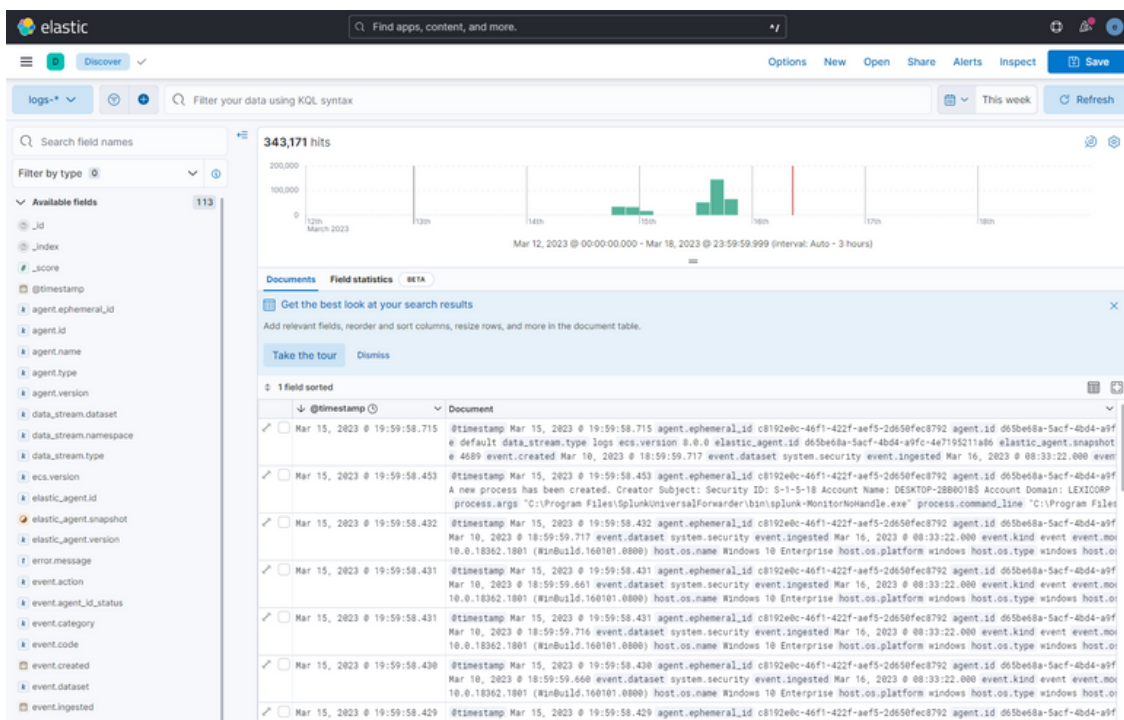


Verify Log Ingestion

- Once in the 'Discover' section of Kibana, change the index from metrics-* to logs-*
- Then change the datetime setting to 'This Week'.



- Monitor the ingestion process, logs will continue to stream in until the script is complete.

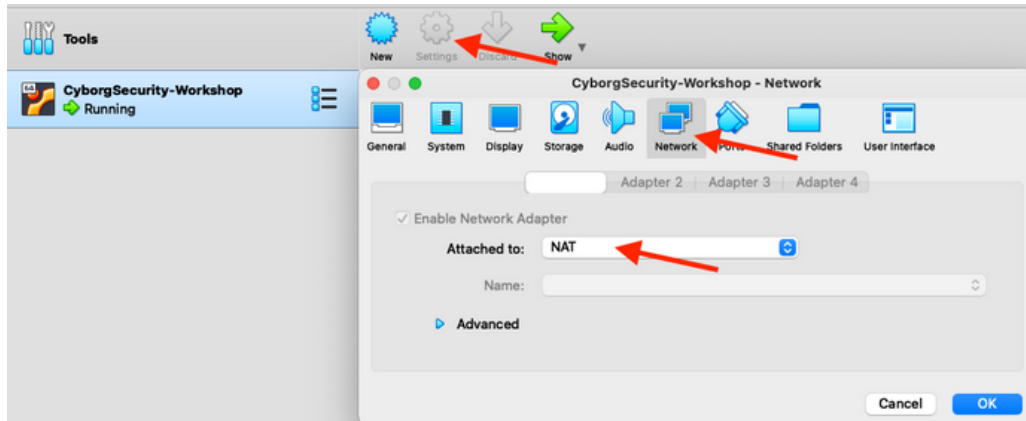


Once the ingestion process is complete there should be 382,621 logs available in Kibana using the 'Today' date setting.

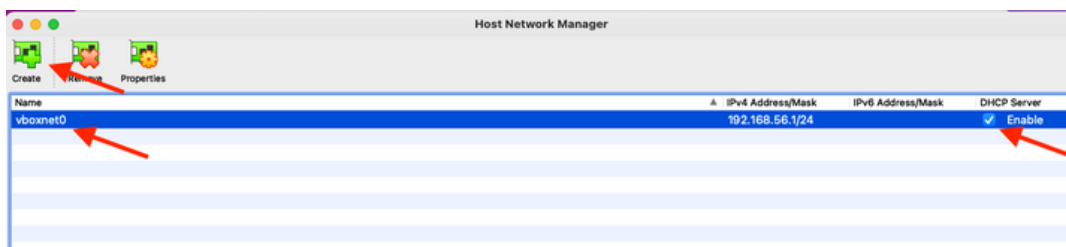
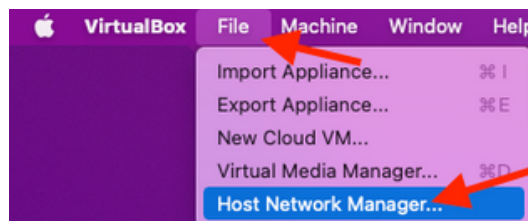


MacOS Networking Workaround - No 'Bridged Networking' over WiFi

- Launch the Virtual Machine with the network settings as NAT, so that the Workshop Log file can be downloaded.
- Log in to the Workshop VM, and follow the steps on page 08 to download and unzip the log files.



- Shutdown the VM and create a 'Host-Only' Adapter.



- Assign the 'Host-Only' adapter and start the Virtual Machine.

