

# THREAT HUNTING WORKSHOP

Hunting for Initial Access

---

Configuration Guide v1.3



Dear students,

As we gear up for an exciting and insightful journey threat hunting, I am thrilled to welcome you to our comprehensive training session. Whether you're a seasoned threat hunter, a dedicated SOC analyst, or an eager cybersecurity professional, this training session is designed with you in mind.

Our mission is to guide you through the entire threat hunting process, offering both theoretical and practical knowledge essential for your growth in the cybersecurity field. We will explore threat hunting and the tools and methodologies that fuel efficient threat hunting.

I hope you're as excited as I am to dive into the world of threat hunting, working with intel reports, crafting hypotheses, planning and executing hunts, and documenting your findings. The key takeaways from this session will help you understand how to develop a solid threat hunting plan, think like a threat hunter, and improve your ability to find and document relationships in data.

This training session is not an introductory course, but a foundation-building experience to refine your existing skills and introduce you to a repeatable process that you can implement in your threat hunting journey. The prerequisites are a laptop that meets the requirements mentioned, your preferred PDF and Excel editors, and a registered community account on the HUNTER platform for enhanced experience.

Remember, it's your curiosity, dedication, and pursuit of knowledge that will drive your success in this session. Let's uncover the mysteries of cybersecurity together and build our capabilities to face the evolving threat landscape.

All the Best,



**Lee Archinal**

Senior Threat Hunter

Cyborg Security

[larchinal@cyborgsecurity.com](mailto:larchinal@cyborgsecurity.com)



## 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.

## 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

Please note, our virtual machine image **now supports** Apple Silicon based chipsets (including the M1, M2, and M3 chipsets).



## 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.



## A Few Notes Before you Begin

### How This Guide Is Broken Down

We know you are anxious to get started, however before you begin to get your environment configured, there are a few important points to note.

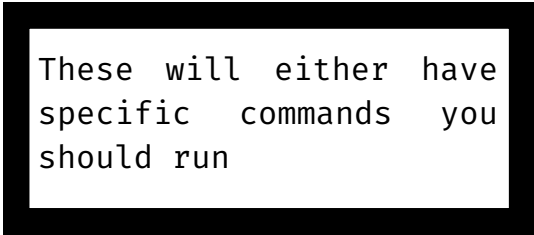
First, this guide is broken down by chipset type, either x86 or Apple Silicon. We have not tested this setup on other platforms (such as other ARM-based chipsets), and while you are welcome to try those, please understand that we **cannot guarantee any functionality in untested platforms.**

If you are using **x86-based processors** (such as most Intel-based and AMD-based processors) start at page 5, with the section "Support for x86-Based Chipsets."

If you are using **Apple Silicon-based processors** (such as the M1, M2 or M3 processors) continue until page 9, "Support for Apple Silicon-based Chipsets."

### Useful Conventions

You'll see callout boxes used throughout this guide



```
These will either have  
specific commands you  
should run
```

or



```
Important information highlighted for you
```



# Step 1 – Get Your HUNTER Account!

We'll be using The HUNTER threat hunting content platform extensively throughout this training session. Set up your account using the easy steps below.

**Already have a HUNTER Account? No problem, you're all set - we've applied the promo code below to your account!**

Head over to [hunter.cyborgsecurity.io](https://hunter.cyborgsecurity.io) and click "Sign Up!"

Fill out your details in the form. **Please note, we do require a valid business email address for identity verification purposes.** Under the promocode enter:

INITIALACCESS

Your account should be created within 1 business day. Please note weekends and holidays may affect this.



## Support for x86-Based Chipsets

### Step 1 - Download the Virtualization Platform

If you are using an x86-based chipset you will need to install VirtualBox on your system. VirtualBox is free to use, and can be downloaded using the link below:

[Download Here](#)

### Step 2 - Download & Load the Environment

You will need to download the Virtual Machine (OVA) we have designed for this course.

The virtual machine can be downloaded here:

`https://huntwithcyb.org/3LKAWMb`

Next, open the VirtualBox virtualization environment, and select

`File ⇨ Import Appliance`

Then, select the downloaded OVA. Select the 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.

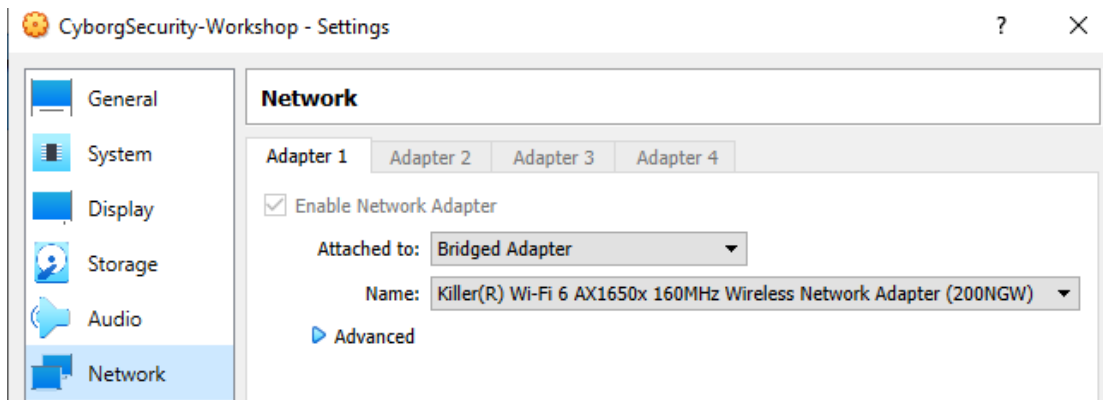
Press 'Import' once the configuration options are approved.



## Step 3 - Configure the Networking

### Configure the Workshop Virtual Machine's Networking

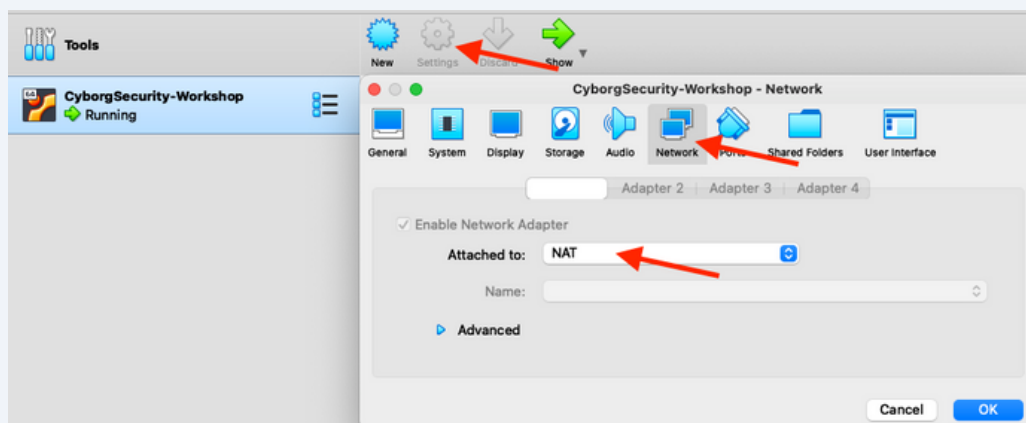
- Go to 'Machine' ⇒ 'Settings' and select the Network Tab.
- Change the 'Attached to:' setting to select the 'Bridged Adapter'.
- Press 'OK' once complete
- If you are a macOS user and are experiencing difficulty, see "macOS Networking Workaround" below, if not, skip to Step 4.



### macOS Networking Workaround - No 'Bridged Networking' over WiFi

If you are a macOS user on an x86 platform, and are experiencing difficulties with networking, follow the following steps for a macOS networking workaround for No Bridged Networking over WiFi.

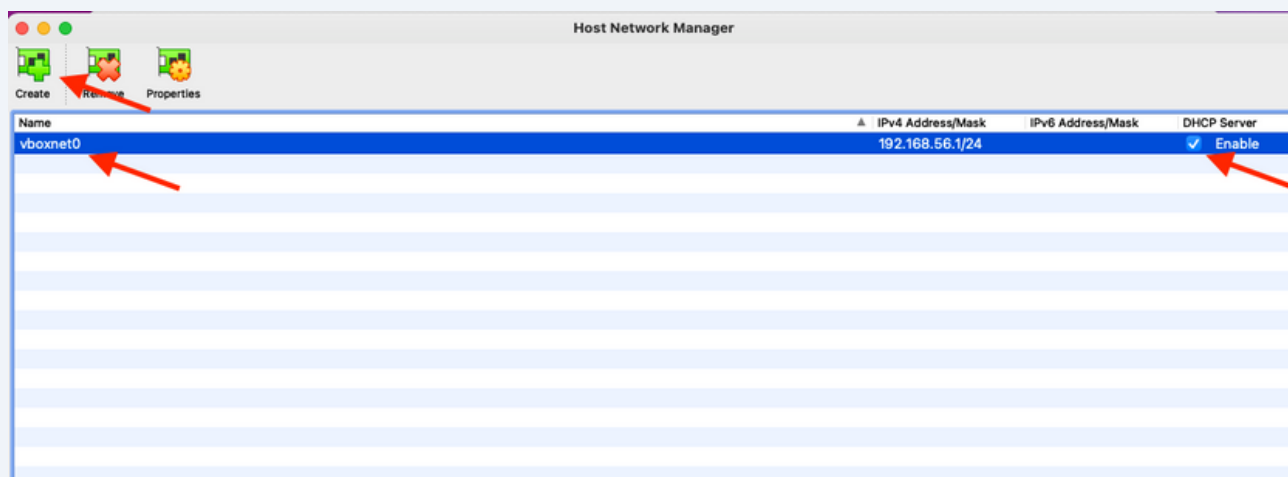
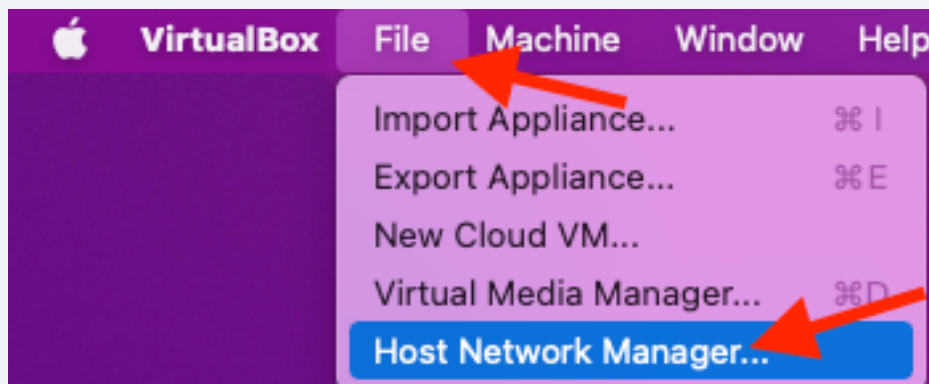
Launch the Virtual Machine with the network settings as NAT, so that the Workshop Log file can be downloaded.



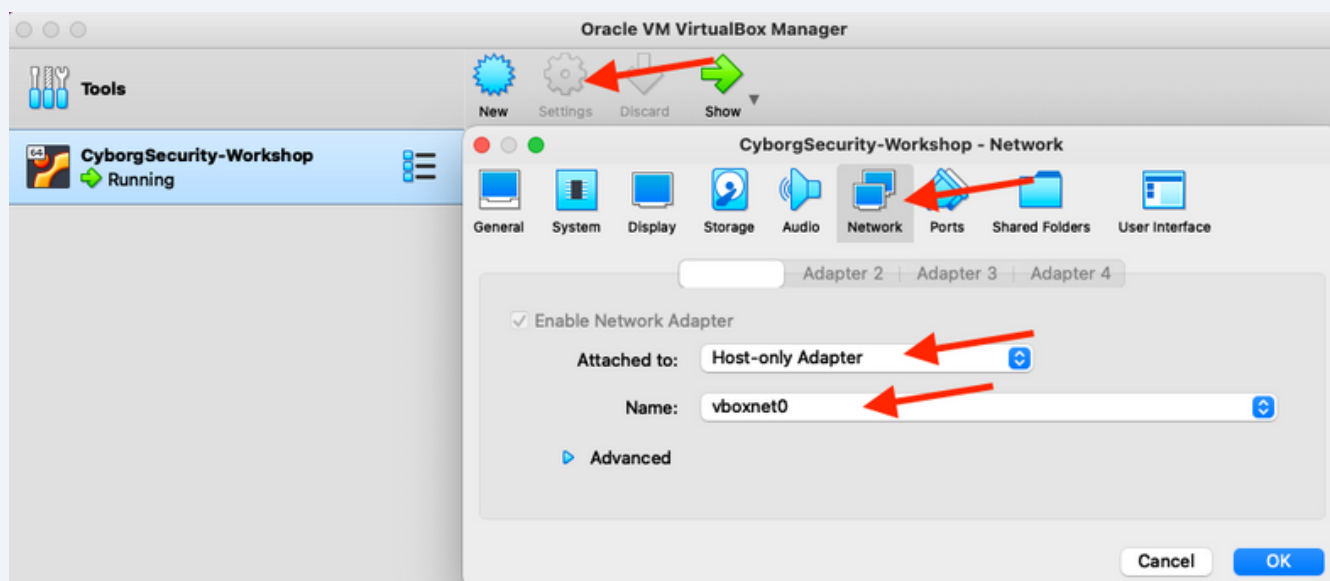




Shutdown the VM and create a 'Host-Only' Adapter.



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

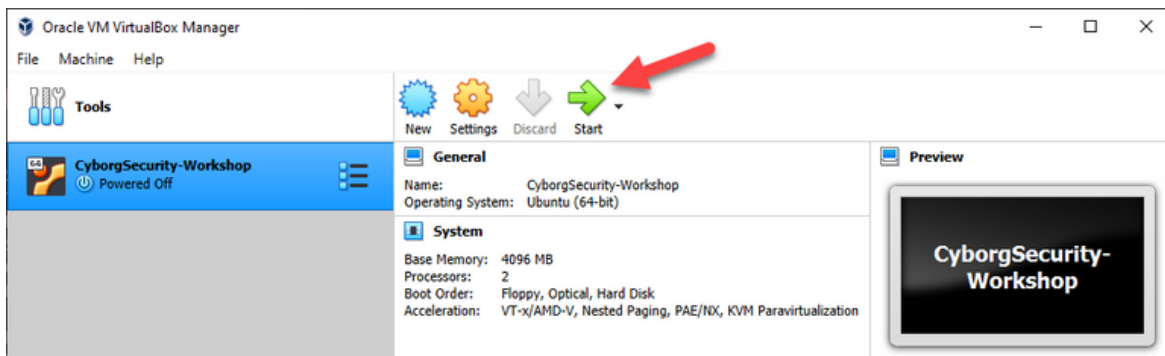




## Step 4 - Start the Environment

### Start and login the Workshop Virtual Machine

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





## Support for Apple Silicon-based Chipsets

### Step 1 - Download the Virtualization Platform

If you are using an Apple Silicon-based chipset (including both M1, M2, or M3), you will need to download a copy of VMWare Fusion (either the 30 day trial of VMWare Fusion or the Personal Use License for VMWare Fusion Player)

[Download Here](#)

### Step 2 - Download & Load the Environment

You will need to download the Virtual Machine we have designed for this course.

The virtual machine can be downloaded here:

```
https://cyborg-pub.s3.us-east-2.amazonaws.com/Workshop/CyborgSecurity-Workshop-ARM.zip
```

You will then need to decompress the virtual machine using the command:

```
unzip CyborgSecurity-Workshop-ARM.zip
```

Double click the uncompressed virtual machine to load it into VMWare Fusion. When VMWare Fusion asks whether the file has been "Moved" or "Copied" select:

```
I Copied It
```



## Logging Into Your Virtual Machine

Log into your virtual machine using the following credentials

```
Username: workshop  
Password: Cyb0rgW0rksh0p!
```

Note: these credentials are **only for logging into the Virtual Machine, not for logging into Kibana/ElasticSearch.**

## Configuring Your Virtual Machine

### File Locations

ElasticSearch and Kibana are managed by Docker and Docker-Compose files found in the following location:

- /home/workshop/workshop

### Checking the Services

To check the Elasticsearch and Kibana services use the following steps:

```
cd /home/workshop/workshop  
  
sudo docker-compose ps
```



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'.

If those services are in a 'DOWN' state, try rebooting the virtual machine.

```
rkshop@workshop-elastic:~/workshop$ sudo docker-compose ps
[sudo] password for workshop:

```

Name	Command	State	Ports
rkshop_elasticsearch_1	/bin/tini -- /usr/local/bi	Up (healthy)	0.0.0.0:9200->9200/tcp,:
	...		200->9200/tcp, 9300/tcp
rkshop_kibana_1	/bin/tini -- /usr/local/bi	Up (healthy)	0.0.0.0:5601->5601/tcp,:
	...		601->5601/tcp

Confirm the IP address of your virtual machine by running 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
```



## Downloading the Data into Your Environment

From *within* your virtual machine, download the new log files using the command (note this should all appear on a single line when copied):

```
wget https://cyborg-pub.s3.us-east-2.amazonaws.com/Workshop/HuntForInitialAccess.tar.gz
```

Then change your working directory to the “workshop” folder and untar (uncompress) the downloaded files

```
cd /home/workshop  
tar zxvf HuntForInitialAccess.tar.gz
```

This process will create a file entitled ‘HuntForInitialAccess.tar.gz’ in the current directory.

## Loading the Data

### Ingesting the Logs

Run the following commands sequentially to start the log ingestion process by indexing the .ndjson file created in the previous step into your ElasticSearch instance.

```
cd /home/workshop/  
  
python3 ingest_logs.py /home/workshop/HuntForInitialAccess.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.



## Accessing Your Hunting Environment

In order to access Kibana, the web-based interface to ElasticSearch, use the following steps:

Open a web browser, and in the address bar enter the following, replacing <IP ADDRESS> with the address you identified in the previous step:

```
http://<IP ADDRESS>:5601
```

From there you will be prompted to login. Use the following credentials.

```
Username: elastic  
Password: Cyb0rgW0rksh0p!
```

**Note: these credentials are only for logging into Kibana/ElasticSearch, these will not work to log into the Virtual machine.**



Once authenticated, open the side drawer and click on the 'Discover' option

