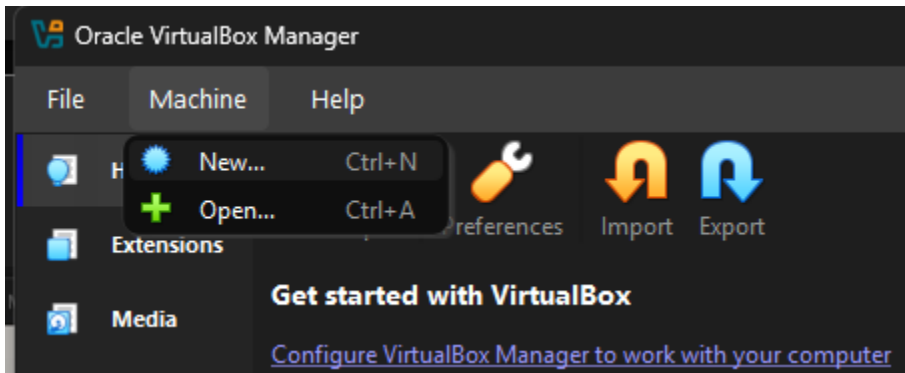


BluevsRed-bootcamp VM Setup Guide

VM User ID: ignitecyber Password: password

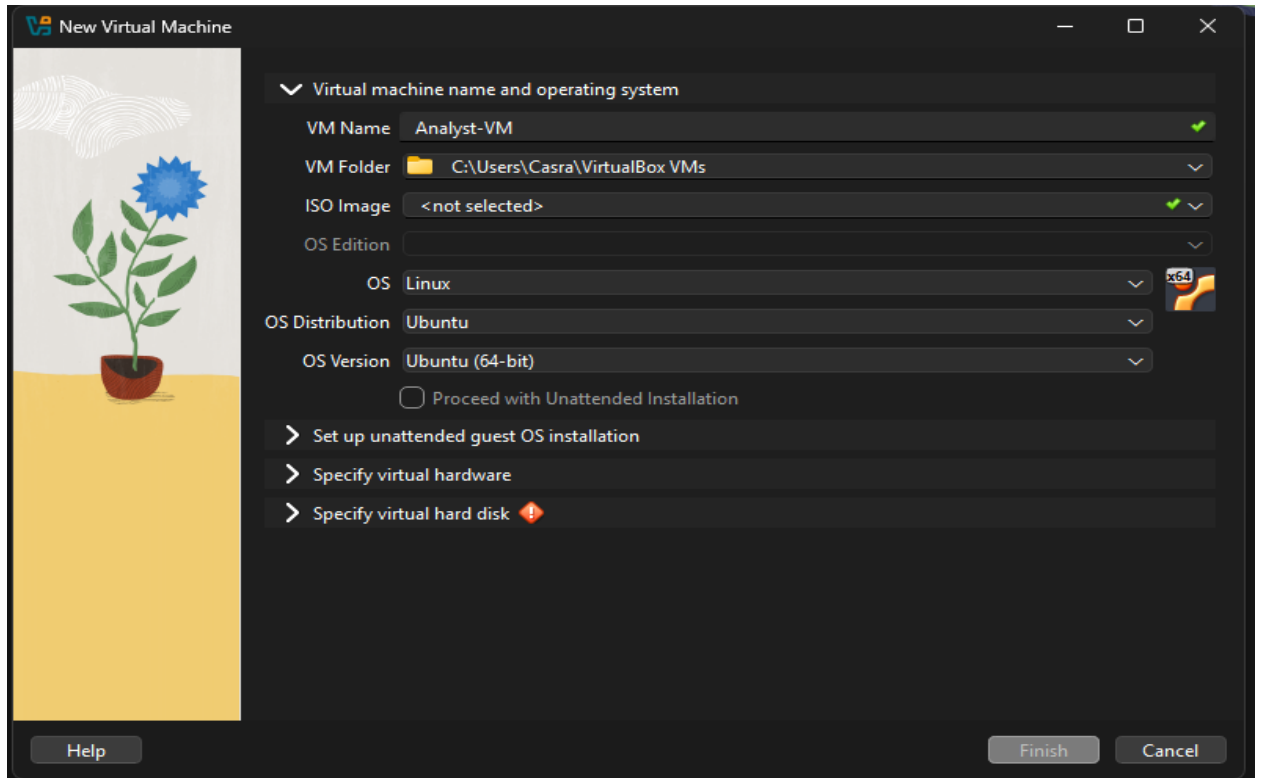
1. Creating the Virtual Machine on VirtualBox

1. Unzip the vdi.zip files.
Optionally: For Mac, open the file with [Keka](#) to make the process faster.
2. In VirtualBox, select Machine > New



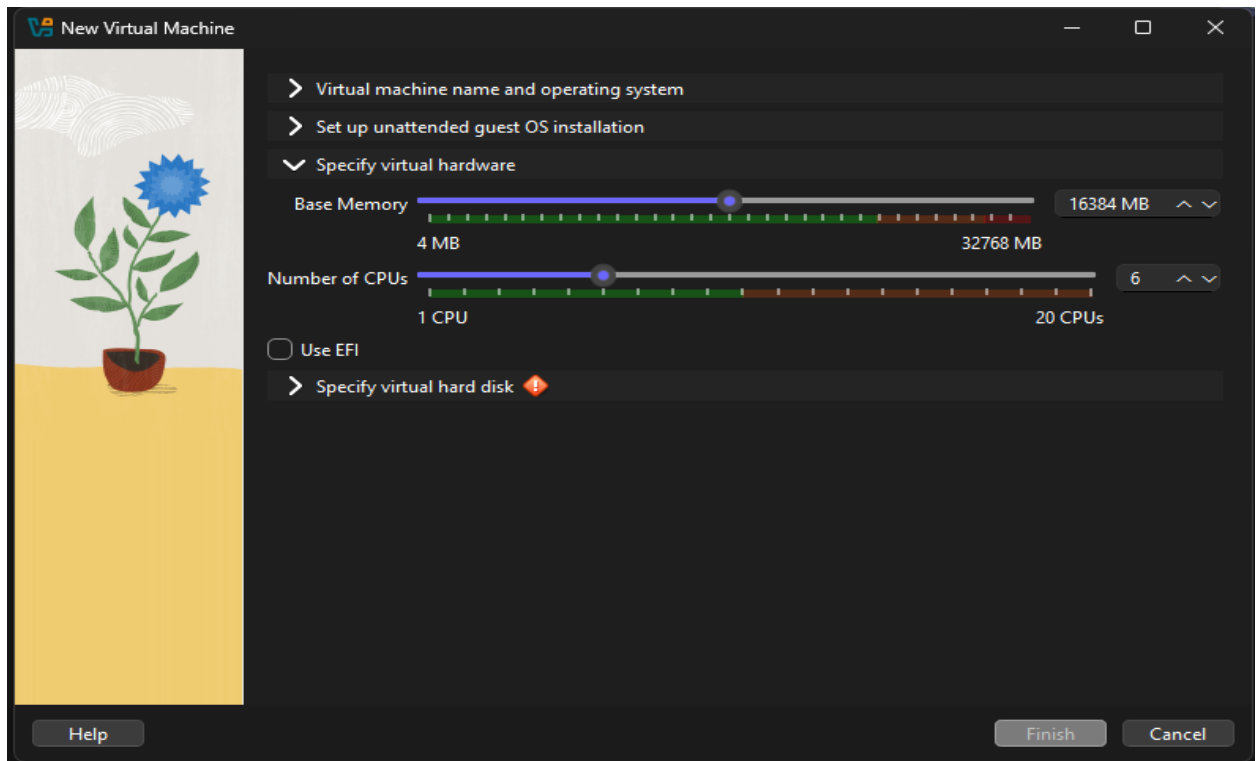
- 3.
4. Depending on the VM, select the following:

	Analyst VM	Red VM
Name	Analyst VM	Red VM
Type	Linux	Linux
Subtype	Ubuntu	Debian
Version	Ubuntu (64-bit)	Debian (64-bit)

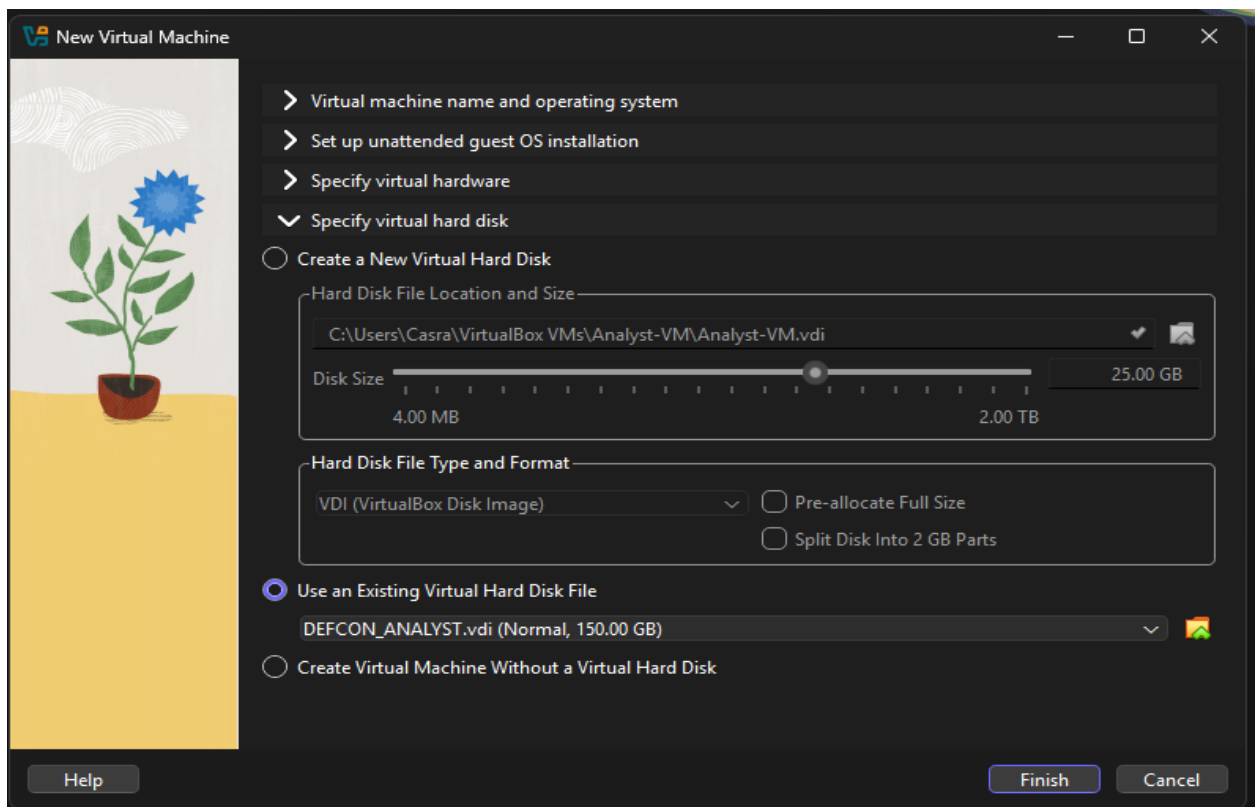


5. Depending on the VM, select the following Hardware values:

	Analyst VM	Red VM
Processor (Minimum - Recommended)	6CPU - 8CPU	2CPU - 4CPU
RAM (Minimum - Recommended)	24576 MB – 32768 MB	4096 MB – 8192 MB



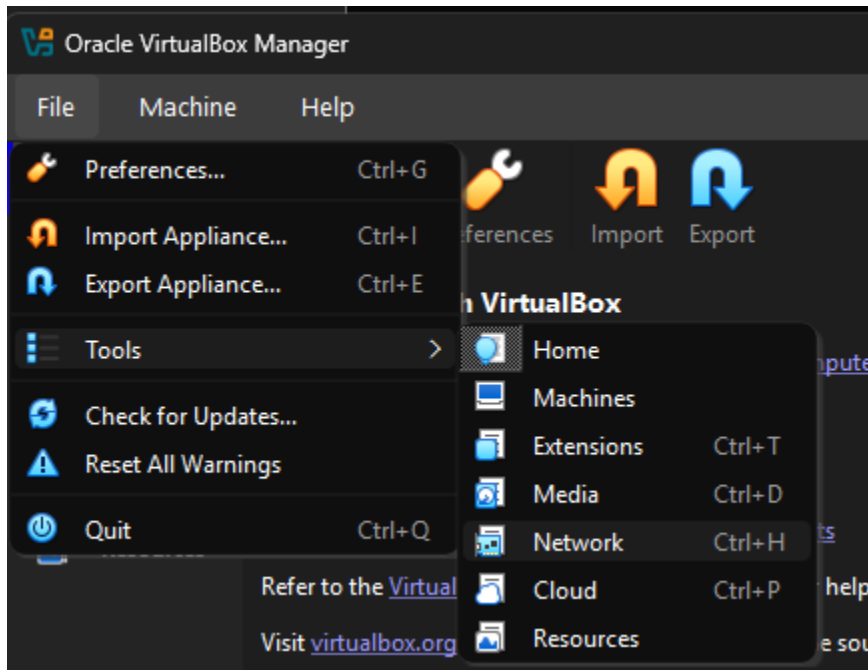
6. For Hard Disk, select “Use an existing Hard Disk File” and browse to the unzipping location for the DEFCON_ANALYST.vdi or RED_VM.vdi.



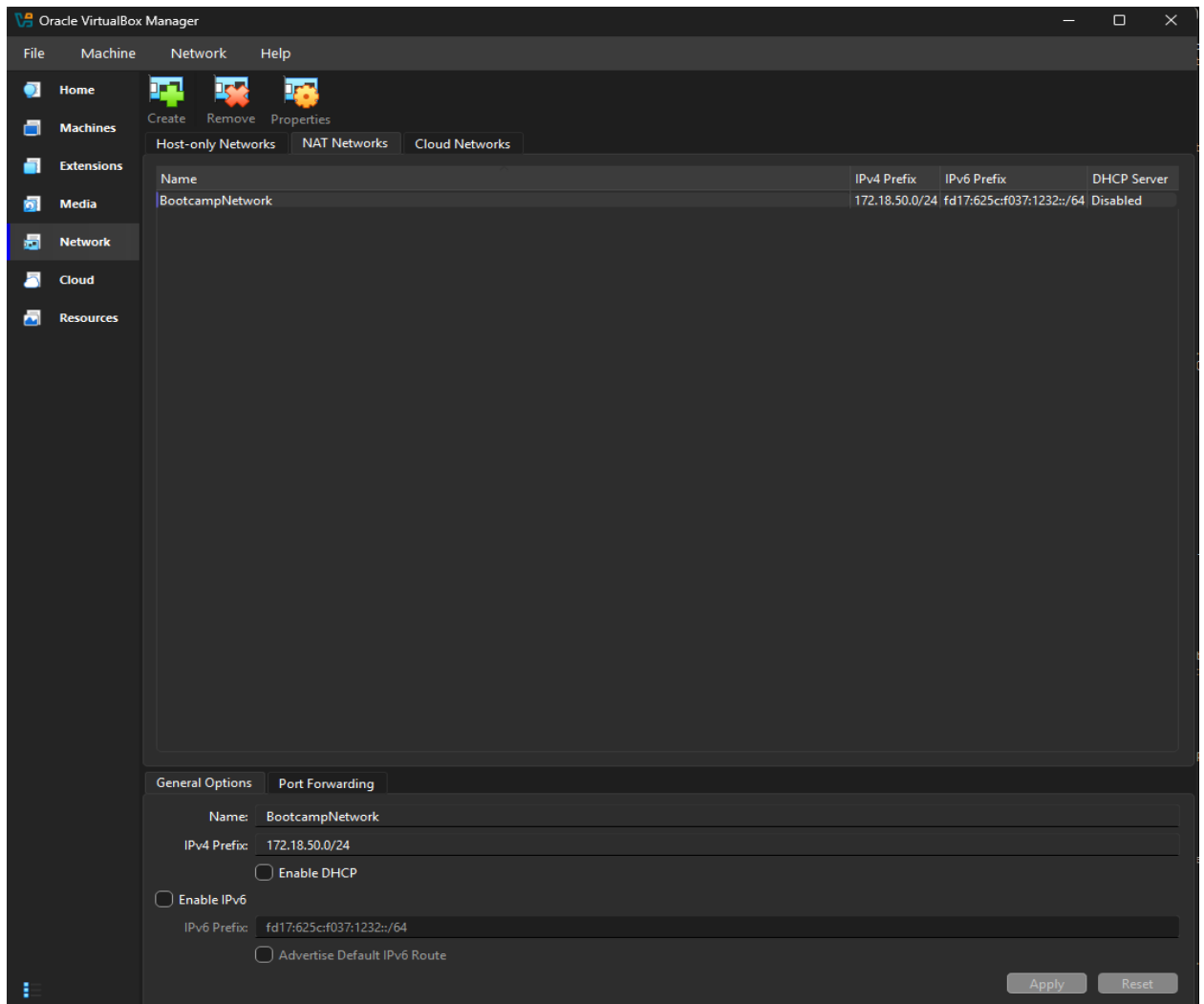
7. Click Finish.
8. Repeat for the other VM.

2. Creating the Subnet

1. From the VirtualBox File menu, select Tools > Network Manager



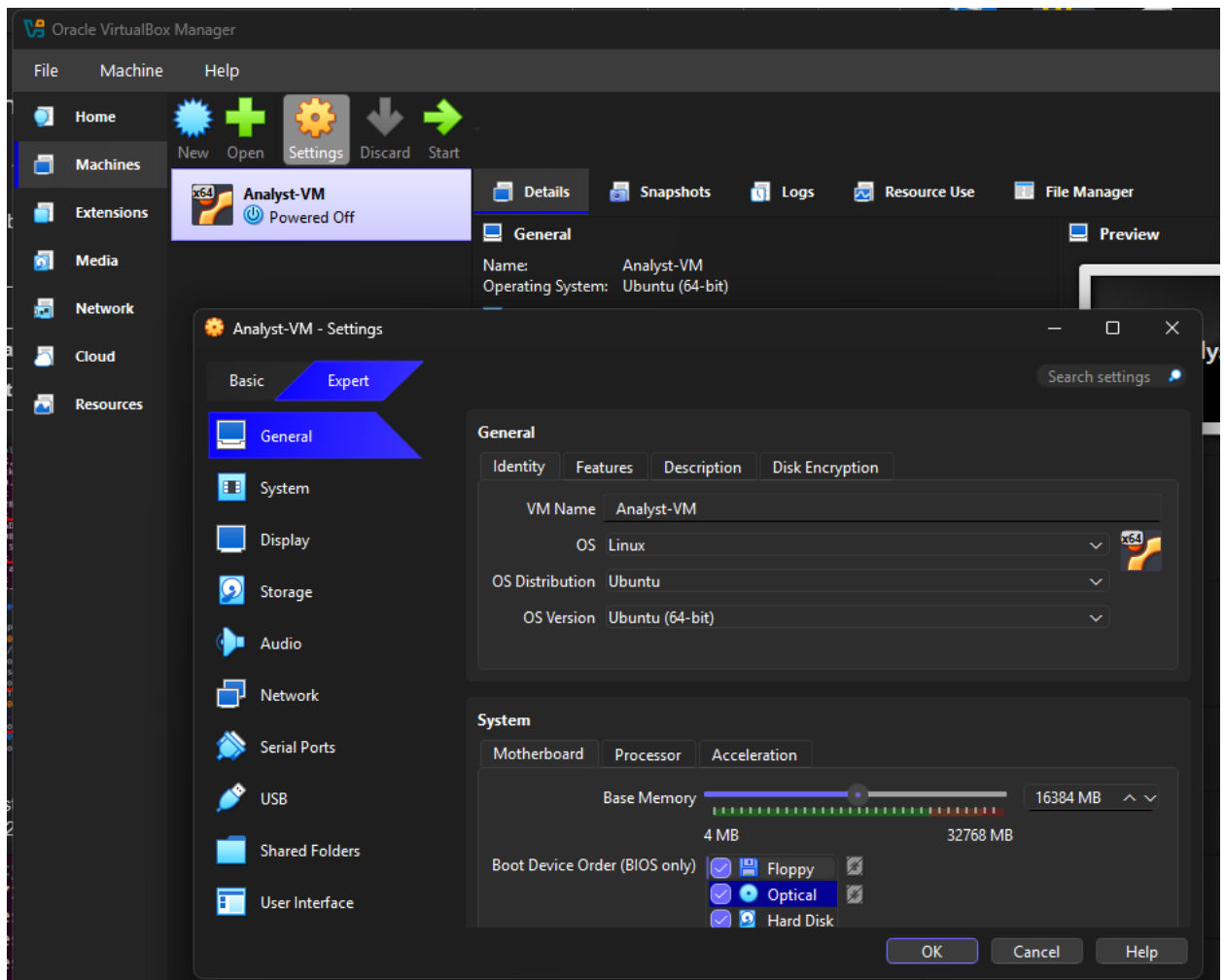
2. Go to NAT Networks and click on Create. Add the following values:
Name: BootcampNetwork
IPv4 Prefix: 172.18.50.0/24
**Ensure the Enable DHCP option is unchecked.*



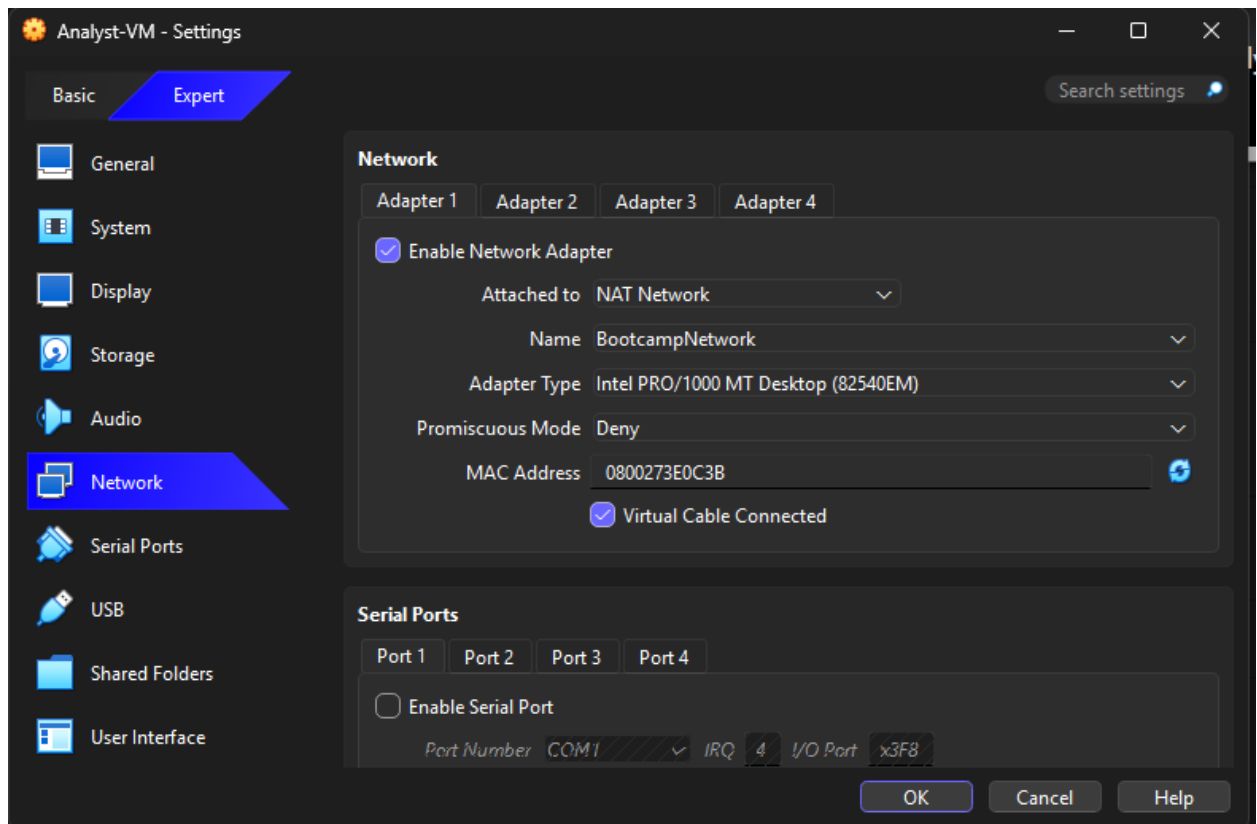
3. Click Apply.

3. Connecting the VMs to the subnet

1. In the VM settings, select Network.



2. Select the following
Attached to: NAT Network
Name: BootcampNetwork



3. Click OK.
4. Repeat for the other VM.

4. Test Connectivity

1. Ensure both VMs are running.
2. Ensure that both VMs have the right IP address by running *ip a*

	Analyst-VM	Red-VM
Interface	enp0s3	eth0
Inet	172.18.50.20/24	172.18.50.30/24

```
ignitecyber@ic-bluevred:~$ 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 08:00:27:8c:37:ee brd ff:ff:ff:ff:ff:ff
    inet 172.18.50.20/24 brd 172.18.50.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8c:37ee/64 scope link
        valid_lft forever preferred_lft forever

ignitecyber@red-vm:~$ 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 noprefixroute
        valid_lft forever preferred_lft forever
2: eno0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:52:2a:67 brd ff:ff:ff:ff:ff:ff
    inet 172.18.50.30/24 brd 172.18.50.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe52:2a67/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

3. From Analyst-VM run:

`ping -c 3 172.18.50.30`

```
ignitecyber@ic-bluevred:~$ ping -c 3 172.18.50.30
PING 172.18.50.30 (172.18.50.30) 56(84) bytes of data.
64 bytes from 172.18.50.30: icmp_seq=1 ttl=64 time=1.58 ms
64 bytes from 172.18.50.30: icmp_seq=2 ttl=64 time=1.58 ms
64 bytes from 172.18.50.30: icmp_seq=3 ttl=64 time=0.756 ms

--- 172.18.50.30 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.756/1.305/1.581/0.388 ms
ignitecyber@ic-bluevred:~$
```

4. From Red-VM run:

`ping -c 3 172.18.50.20`

```
(ignitecyber@red-vm)-[~]
$ ping -c 3 172.18.50.20
PING 172.18.50.20 (172.18.50.20) 56(84) bytes of data.
64 bytes from 172.18.50.20: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 172.18.50.20: icmp_seq=2 ttl=64 time=1.66 ms
64 bytes from 172.18.50.20: icmp_seq=3 ttl=64 time=1.11 ms

— 172.18.50.20 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2385ms
rtt min/avg/max/mdev = 1.113/1.303/1.657/0.250 ms
```

5. Test both VMs' connectivity to the internet and the DNS:

`ping -c 3 8.8.8.8`

```
ignitecyber@ic-bluevred:~$ ping -c 3 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=13.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=13.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=13.9 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 13.081/13.485/13.937/0.351 ms
```

ping -c 3 google.com

```
ignitecyber@ic-bluevred:~$ ping -c 3 google.com
PING google.com (173.194.193.100) 56(84) bytes of data.
64 bytes from iu-in-f100.1e100.net (173.194.193.100): icmp_seq=1 ttl=107 time=24.7 ms
64 bytes from iu-in-f100.1e100.net (173.194.193.100): icmp_seq=2 ttl=107 time=24.6 ms
64 bytes from iu-in-f100.1e100.net (173.194.193.100): icmp_seq=3 ttl=107 time=22.2 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 22.218/23.832/24.689/1.142 ms
```

5. VM Update

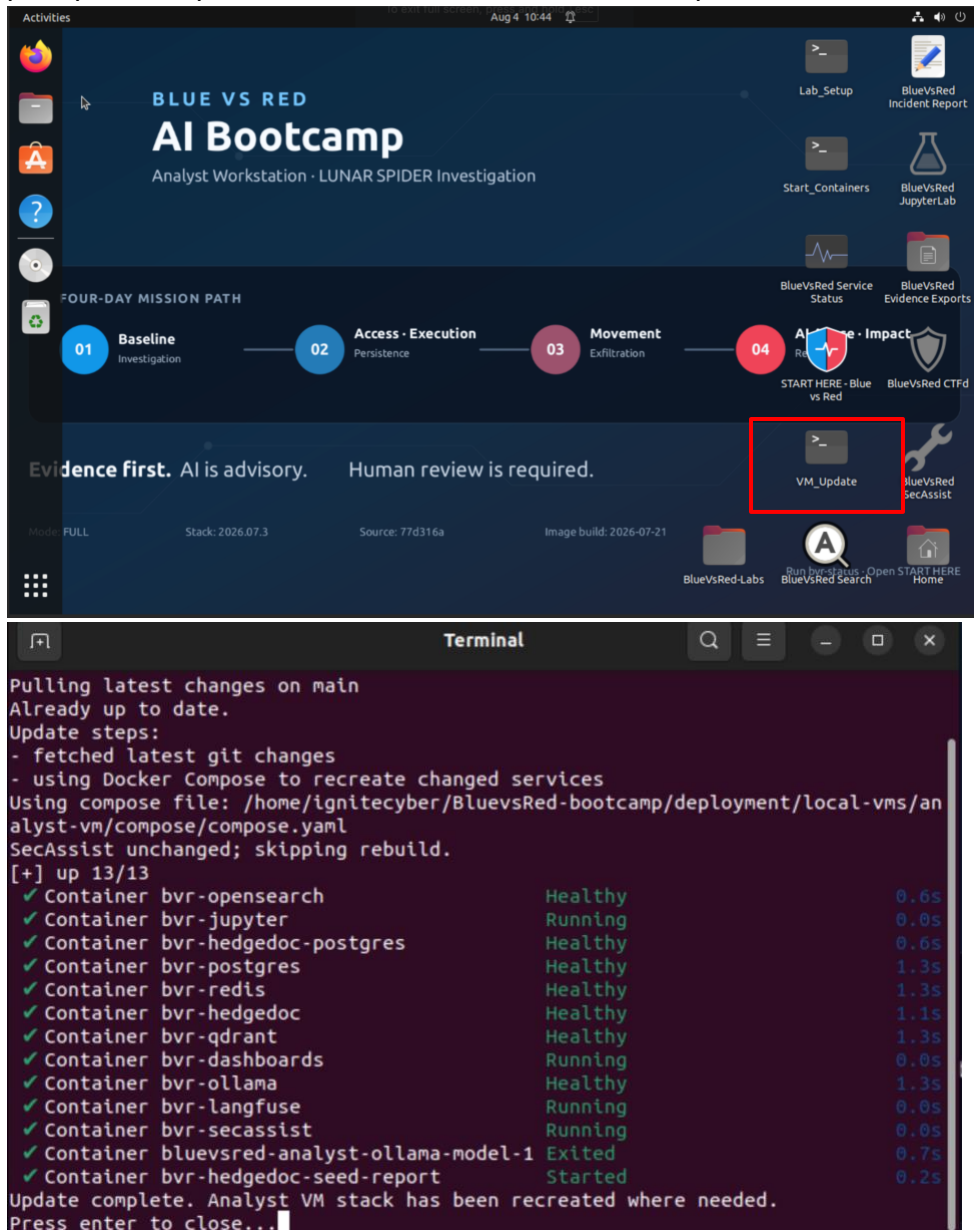
1. On the Analyst_VM, click on Start_Containers and wait for it to complete the run.

The screenshot displays the 'BLUE VS RED AI Bootcamp' Analyst Workstation interface. The main window features a dark blue theme with a central mission path titled 'FOUR-DAY MISSION PATH'. The path consists of four stages: 01 Baseline Investigation, 02 Access - Execution Persistence, 03 Movement Exfiltration, and 04 AI - Impact. The 'Start_Containers' button is highlighted with a red box. Below the mission path, there is a section titled 'Evidence first. AI is advisory. Human review is required.' and a status bar showing 'Mode: FULL', 'Stack: 2026.07.3', 'Source: 77d316a', and 'Image build: 2026-07-21'. The bottom right corner contains several utility icons like 'Lab_Setup', 'BlueVsRed Incident Report', 'Start_Containers', 'BlueVsRed JupyterLab', 'BlueVsRed Service Status', 'BlueVsRed Evidence Exports', 'VM_Update', and 'BlueVsRed SecAssist'.

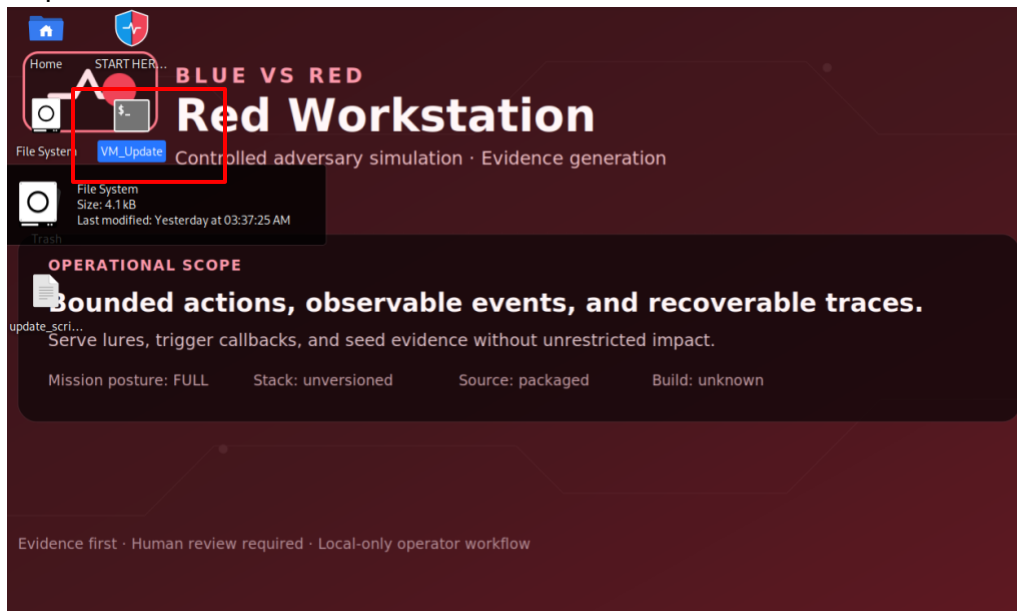
Below the main window, a terminal window titled 'Terminal' shows the output of the 'Start_Containers' command. The output lists 14 containers and their status, along with the time taken for each to start or exit.

```
Starting the containers
[+] up 14/14
✓ Network bluevsred-analyst          Created      0.1s
✓ Container bvr-jupyter              Started      4.1s
✓ Container bvr-opensearch           Healthy      85.8s
✓ Container bvr-postgres             Healthy      24.9s
✓ Container bvr-redis                Healthy      25.3s
✓ Container bvr-ollama               Healthy      25.3s
✓ Container bvr-qdrant               Healthy      25.3s
✓ Container bvr-hedgedoc-postgres    Healthy      24.9s
✓ Container bluevsred-analyst-ollama-model-1 Exited      25.5s
✓ Container bvr-dashboards           Started      85.3s
✓ Container bvr-hedgedoc             Healthy      50.7s
✓ Container bvr-langfuse             Started      24.2s
✓ Container bvr-secassist            Started      25.6s
✓ Container bvr-hedgedoc-seed-report Started      50.4s
Analyst VM setup complete.
Press enter to close...
```

- Click on the VM-Update shortcut on the Desktop, and enter the VM password if prompted, to update the VM content and run the setup.

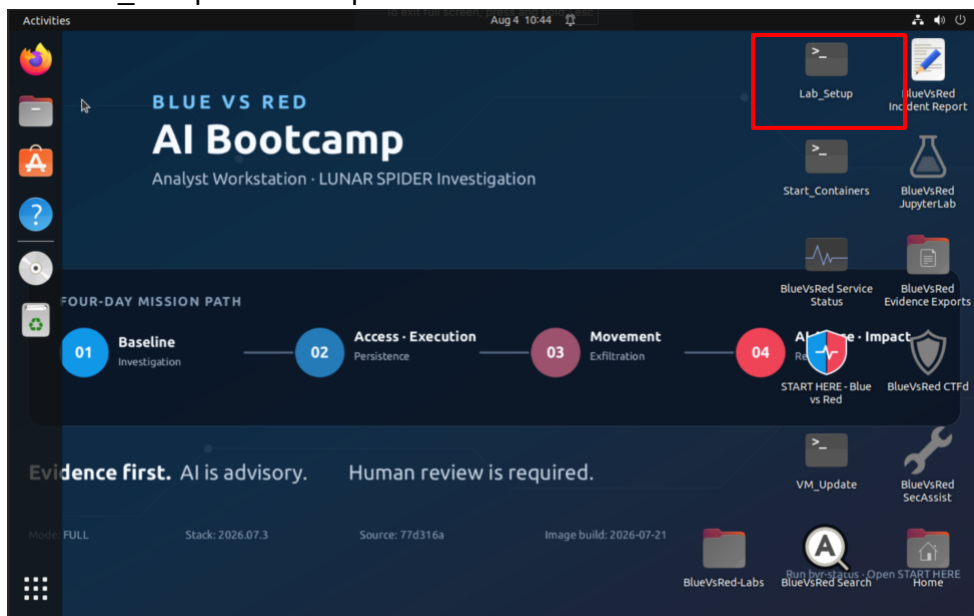


3. Repeat for the Red-VM.



6. Lab Setup

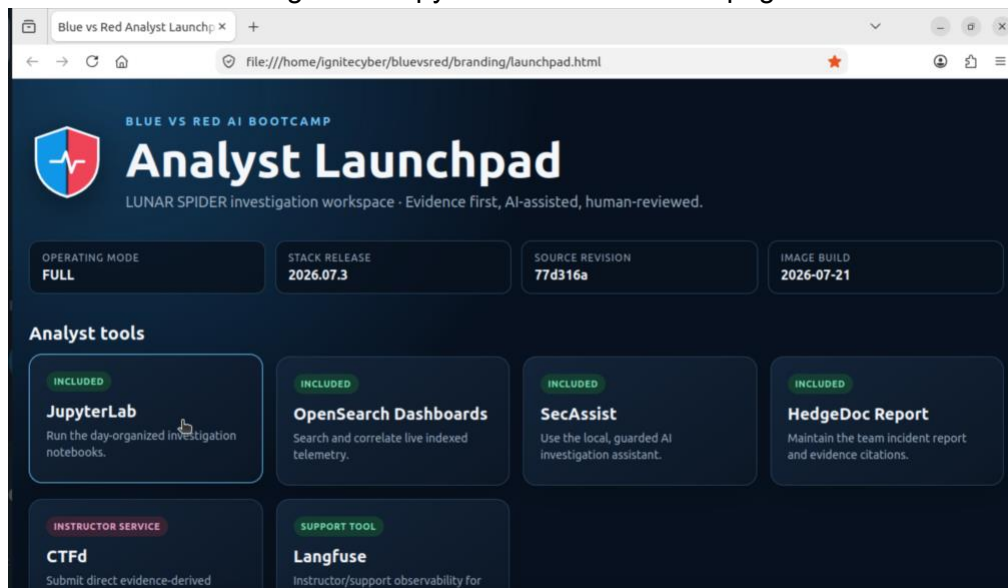
1. Run Lab_Setup on Desktop.



2. Select the notebook for the required lab.

```
Terminal
Available labs:
0. phase-0-baseline (day1_phase0_baseline_lab.ipynb)
1. phase-1-initial-access (day2_phase1_initial_access_lab.ipynb)
2. phase-2-execution-foothold (day2_phase2_execution_foothold_lab.ipynb)
3. phase-3-persistence-privilege (day2_phase3_persistence_privilege_lab.ipynb)
4. phase-4-lateral-movement (day3_phase4_lateral_movement_lab.ipynb)
5. phase-5-collection-exfiltration (day3_phase5_collection_exfiltration_lab.ipynb)
6. phase-6-ghost-in-the-assistant (day4_phase6_ghost_in_the_assistant_lab.ipynb)
7. phase-7-impact-recovery (day4_phase7_impact_recovery_lab.ipynb)
8. all (all)
Select a lab number: 1
Notebook copied: /home/ignitecyber/Desktop/BlueVsRed-Labs/workspace/day2_phase1_initial_access_lab.ipynb
Prepared lab workspace at /home/ignitecyber/Desktop/BlueVsRed-Labs/workspace
Exports will be written to: /home/ignitecyber/Desktop/BlueVsRed-Labs/exports
Environment file written: /home/ignitecyber/Desktop/BlueVsRed-Labs/workspace/.env
Load it into the Jupyter environment before opening the notebook, e.g. `set -a & source "/home/ignitecyber/Desktop/BlueVsRed-Labs/workspace/.env" && set +a`.
Press enter to close...
```

3. Start Firefox and navigate to JupyterLab from the homepage link.



4. Select the notebook to load.

The screenshot displays the JupyterLab web interface. On the left, a file browser pane shows the directory structure under `/work/notebooks/`. A tooltip is open over the file `day1_phase0_baseline_lab.ipynb`, providing the following details:

- Name: day1_phase0_baseline_lab.ipynb
- Size: 127.1 KB
- Path: work/notebooks
- Created: 8/3/26, 5:55 PM
- Modified: 8/3/26, 5:55 PM
- Writable: true
- Kernel: Python 3 (ipykernel)

The main area on the right shows the notebook content, which includes a title **LAB 1.1 - Onboarding, Health Checks, and Phase 0 Baseline Investigation** and a section titled **Intelligence Brief**. The brief describes the organization as Northbridge Logistics and lists business-critical assets such as customer portals, authentication services, and shipment data.