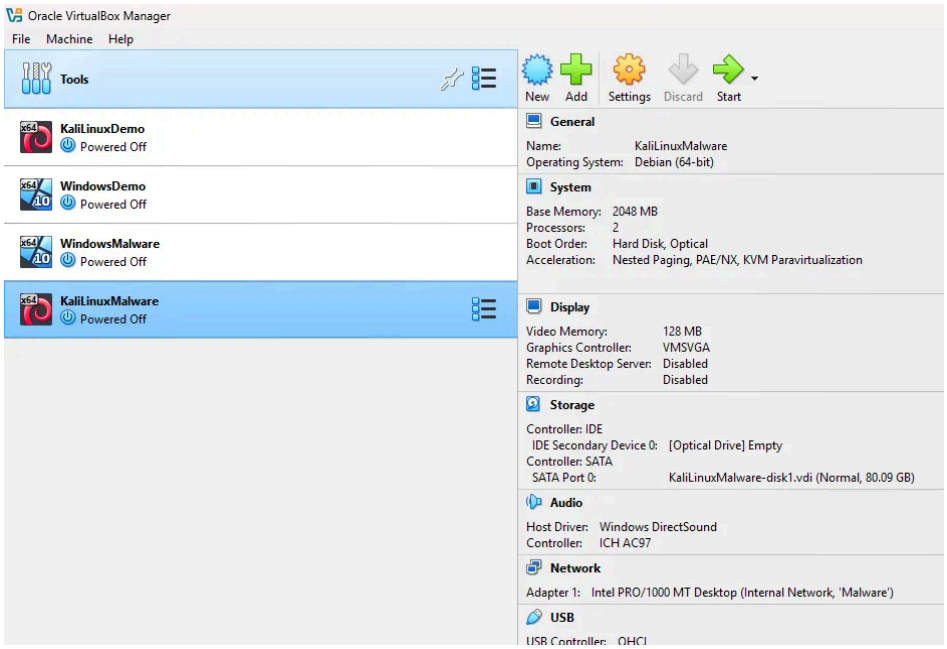
Process

Installing

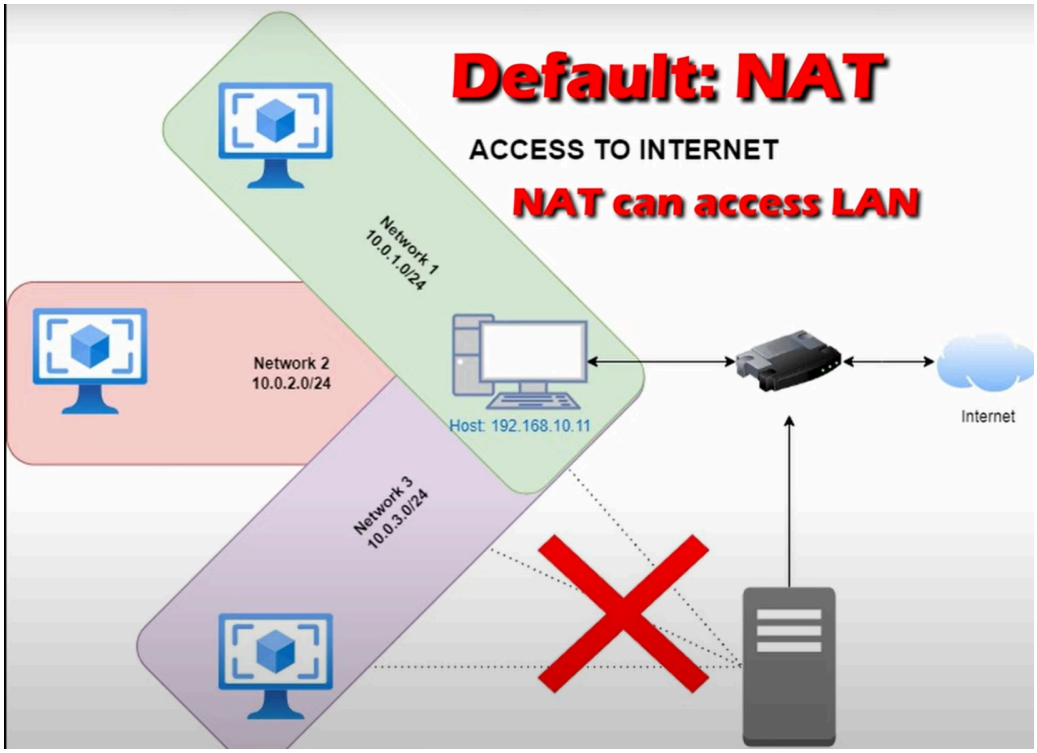
- **Through virtual box** website I have installed the software along and the require other tools (Microsoft Visual C++)
- **Virtual box** - A software that allows you to run different virtual machines or operating systems.
- **VMware** - a company that provides virtualization software, to create virtual machines you can install such as ubuntu. While also having an application similar to VirtualBox
- **Ubuntu** - Provides the interface and functionality for a computer whether its physical or a virtual one. It is a popular Linux distribution, which is a full OS.
- VM Ware is the virtual computer, Ubuntu is like the operating system.
- **Windows 10** - I download an ISO file of **windows 10** to image it to ubuntu, allowing it to run that OS. This acts as the victim machine.
- **Kali Linux** - I download an ISO file of Kali Linux OS to act as the attacker. Kali Linux is better for cybersecurity labs. It comes with preloaded tools and is open source.
    - Penetration Testing (Metasploit, SQLmap)
    - Network analysis (Wireshark, Nmap)
    - Password Cracking (John the ripper, Hashcat)
    - Forensics (Autopsy, Volitity)
    - Wireless Hacking (Aircrack-ng)
- Since companies use windows its important to use a windows OS as the victim
- I am also installing 7 zip, as Kali is a 7 zip file extension
- *Note to self: default Kali credentials are Kali/Kali*



Configuration

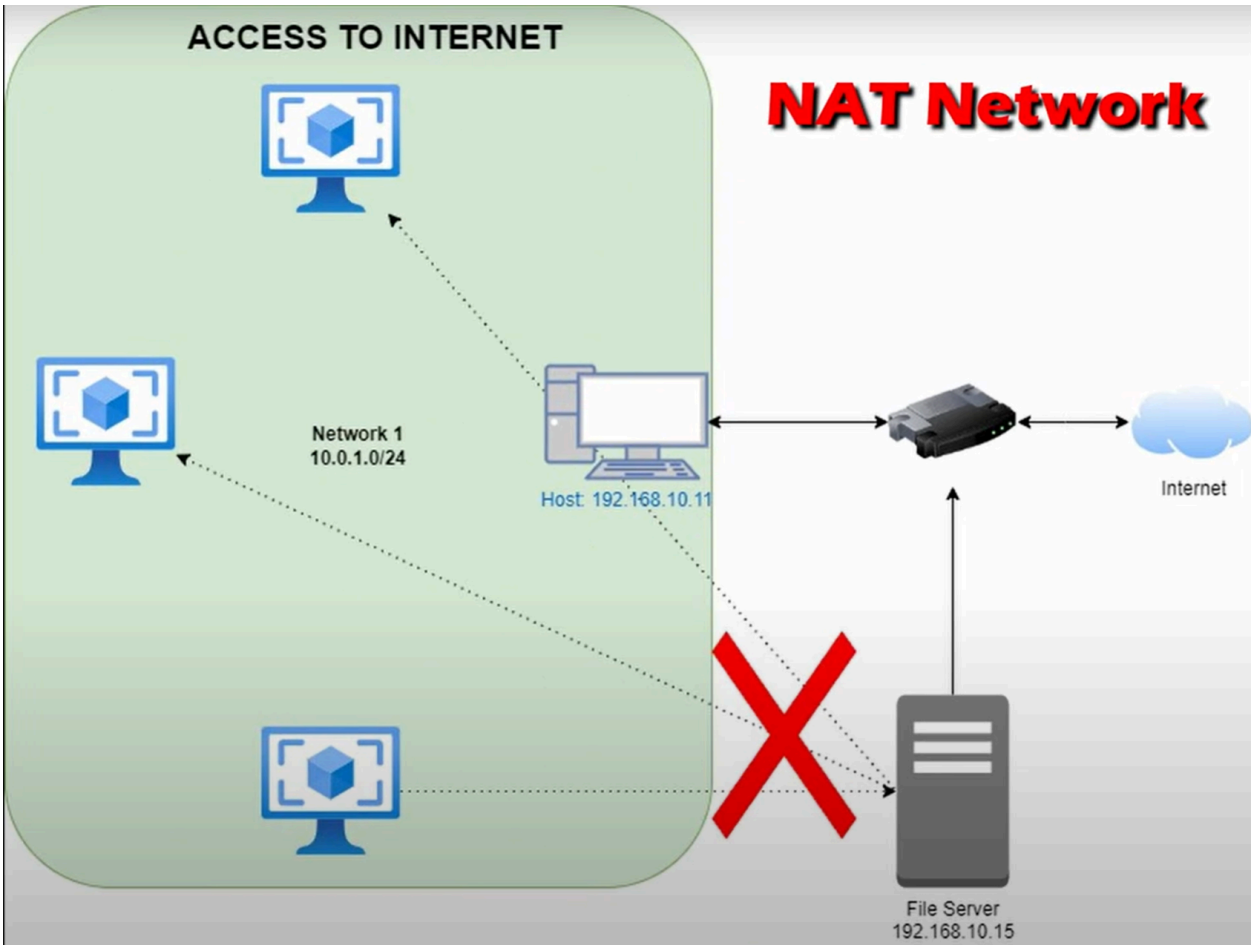
- To properly configure VM Ware and Virtual box, reducing risk when analyzing malware and other tools, it is important to be knowledgeable on different network types
- **NAT** - I am using this network type so I can connect to the internet and each VM is on their own network
- **Not Attached or Internal Network** - using to analyze malware and comprises, so I don't want it to connect to the internet, and I want the VMs to be in its own network
- **Network Options in virtual box include:**

Examples



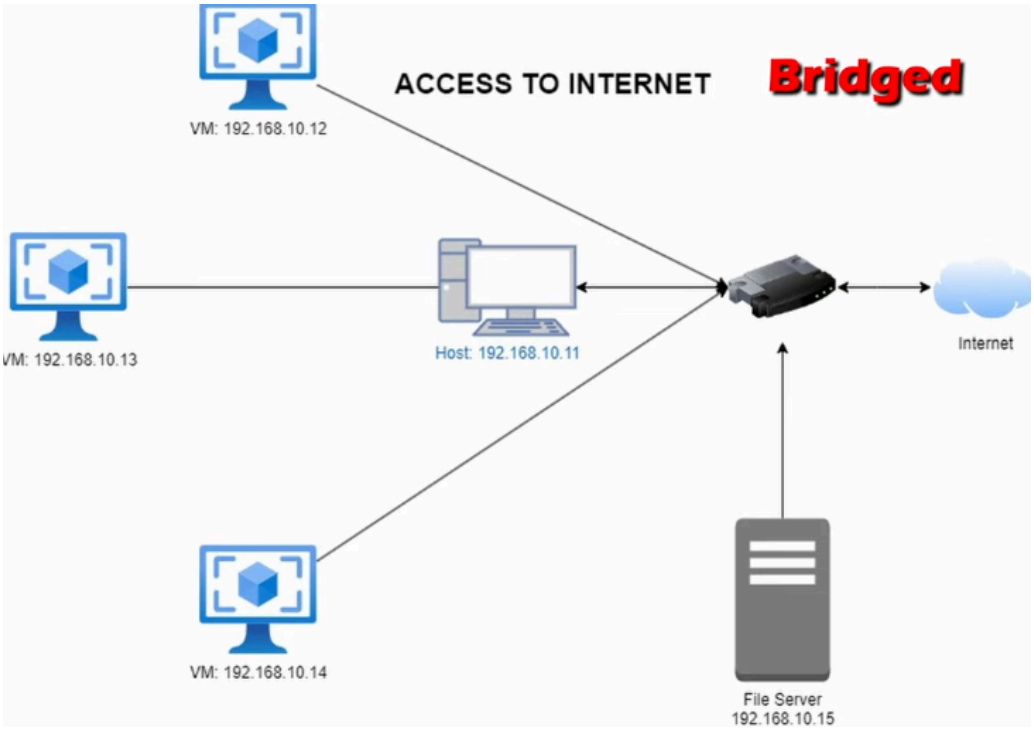
NAT (Network Address Translation) - creates a separate network using the host network adapter and assigns it to each VM

- VM → Host → Router (connects network to internet & Routes local network traffic) → Internet
- Host IP Address: 192.168.10.11
- VM Network 1: 10.0.1.0/24
- VM Network 2: 10.0.2.0/24
- VM Network 3: 10.0.3.0/24
- (Has access to internet & LAN)
- Lan cannot access NAT’s VMS unless port forwarded



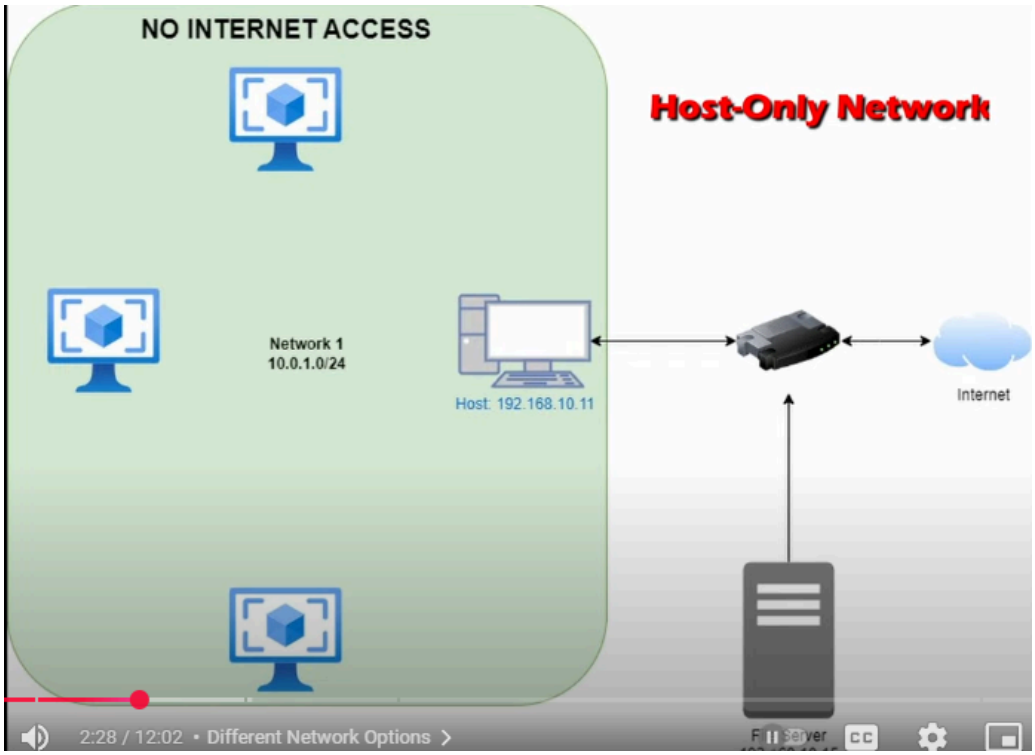
NAT Network - Similar to NAT but instead of three separate networks the VMs will merge into one network

- VM ↔ VM ↔ Host → Router (connects network to internet & Routes local network traffic) → Internet
- Host IP Address 192.168.10.11
- VM Network 1: 10.0.1.0/24
- VM Network 1: 10.0.1.0/24
- VM Network 1: 10.0.1.0/24
- (Has access to internet)



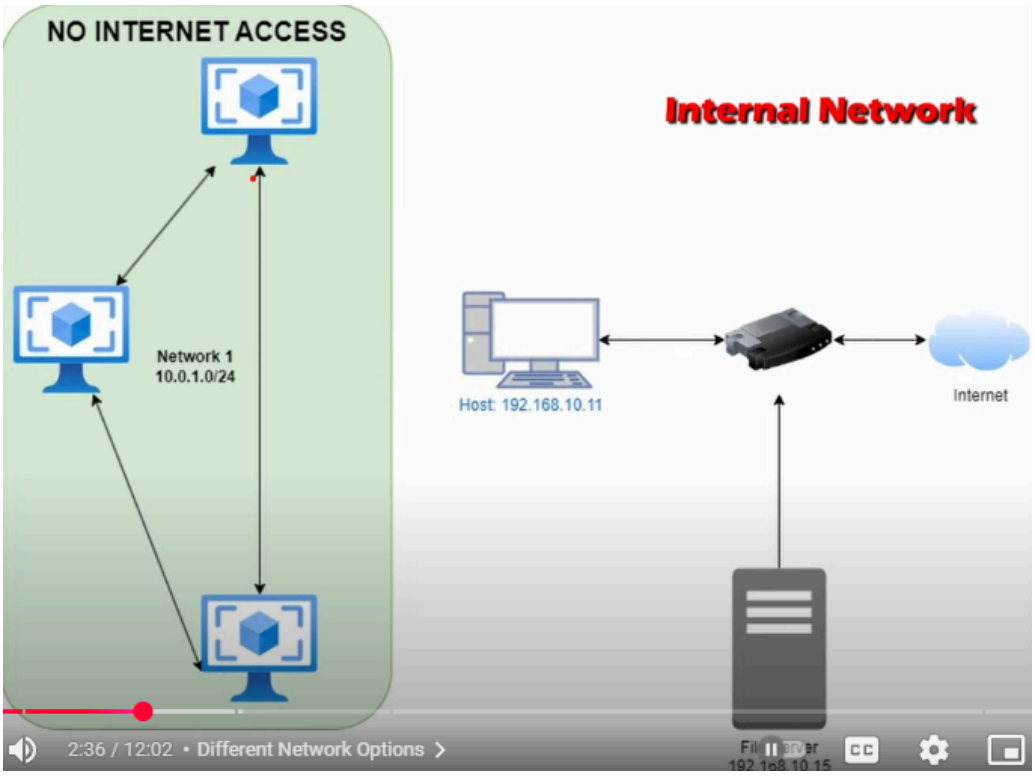
Bridged - This will make your VM act as physical machines meaning same network as your host machine

- EX : Host IP Address 192.168.10.11
- VMs connect straight to internet and router, which can negatively effect your network if malware spreads
- (Has access to internet & LAN)
- We don't want this because we will be running malware and other threat assessment test



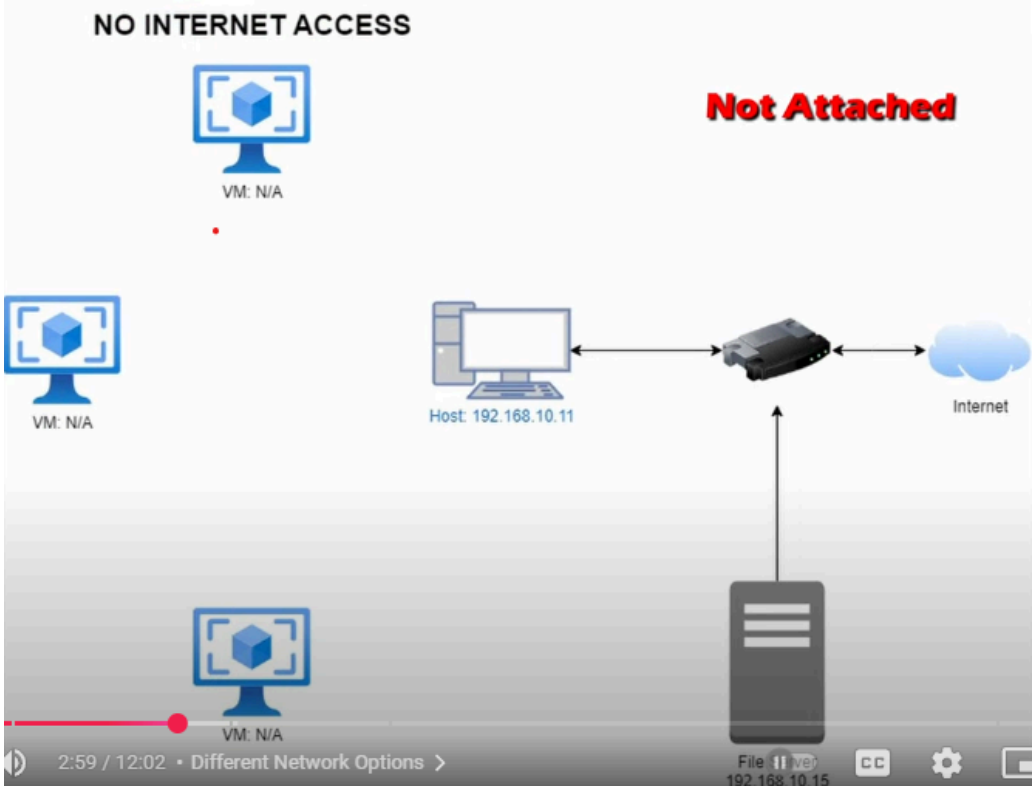
Host-Only Network - VMs are only accessible to the host machine

- (No internet access & LAN)



Internal Network - VMs are in their own separate network

- Typically used for malware analysis
- Each are statically assigned an IP
- (No internet or LAN access)



Not Attached Network - Network adapter isn't attached

There is also Cloud and Generic Networking.