A Practical Approach to Malware Analysis & Memory Forensics

Introduction To Malware Analysis

Who AM I

Monnappa K A

- Over 15 years of Experience in Cyber Security
- Author: Learning Malware Analysis
- Member of Black Hat Review Board
- Co-founder Cysinfo Security Community
- Creator of Limon Sandbox
- Winner of Volatility Plugin Contest 2016
- Presentations & Trainings - Black Hat, FIRST, BruCON, HITB, SEC-T
- Articles - eForensics, Hakin9, Hack Insight

What is Malware?

- Code that is malicious
- Viruses, Worms, Keyloggers, Backdoors, Rootkits

What they do?

- Disrupt computer operation
- Stealing Sensitive information
- Gain access to computer systems
- Spy on computer users

Why Malware Analysis?

- Understand how malware functions
- Determine the nature and purpose of the malware
- Identify network Indicators
- Host-based Indicators
- Determine the persistence mechanism

Types of Malware Analysis

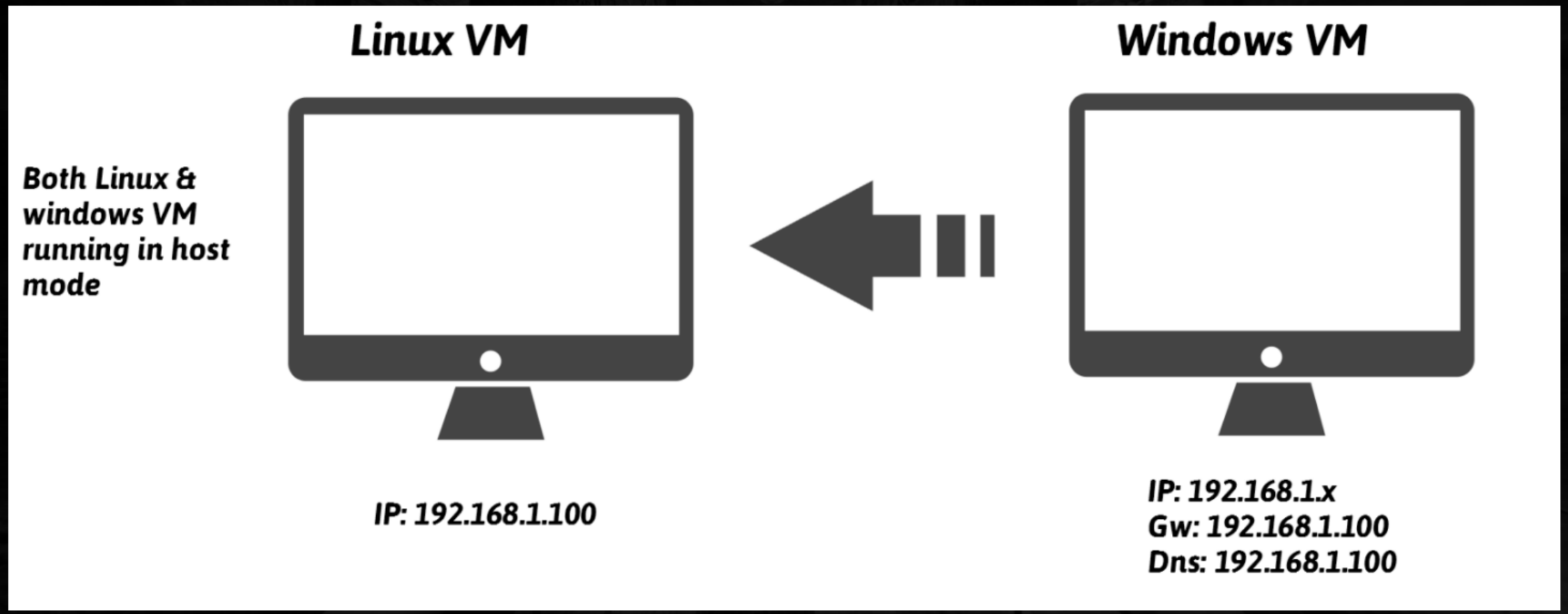
Analysis without executing the malware

Analysis by executing the malware

Analysis of RAM (main memory) after executing the malware

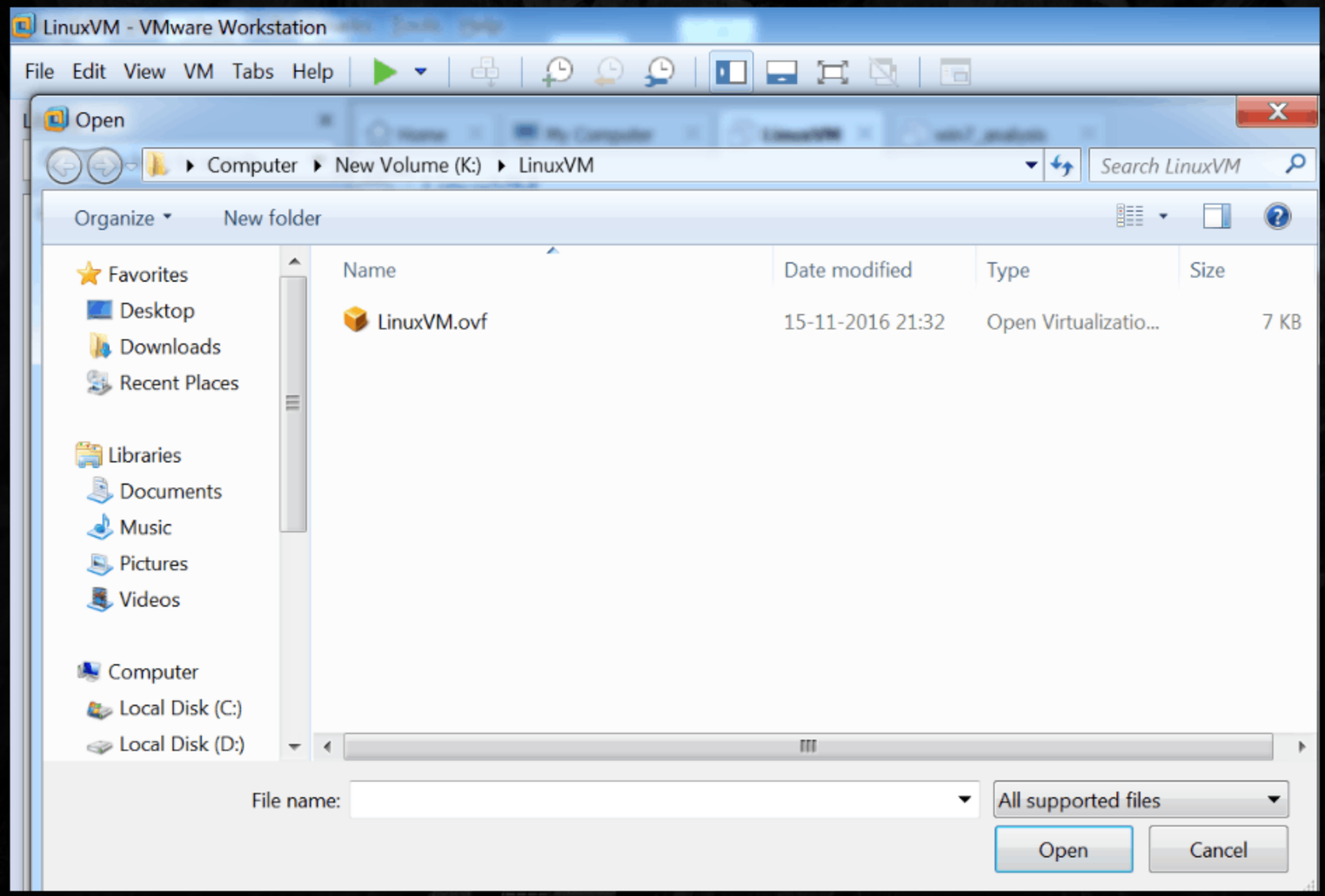
Setting up the Lab Environment

Lab Architecture

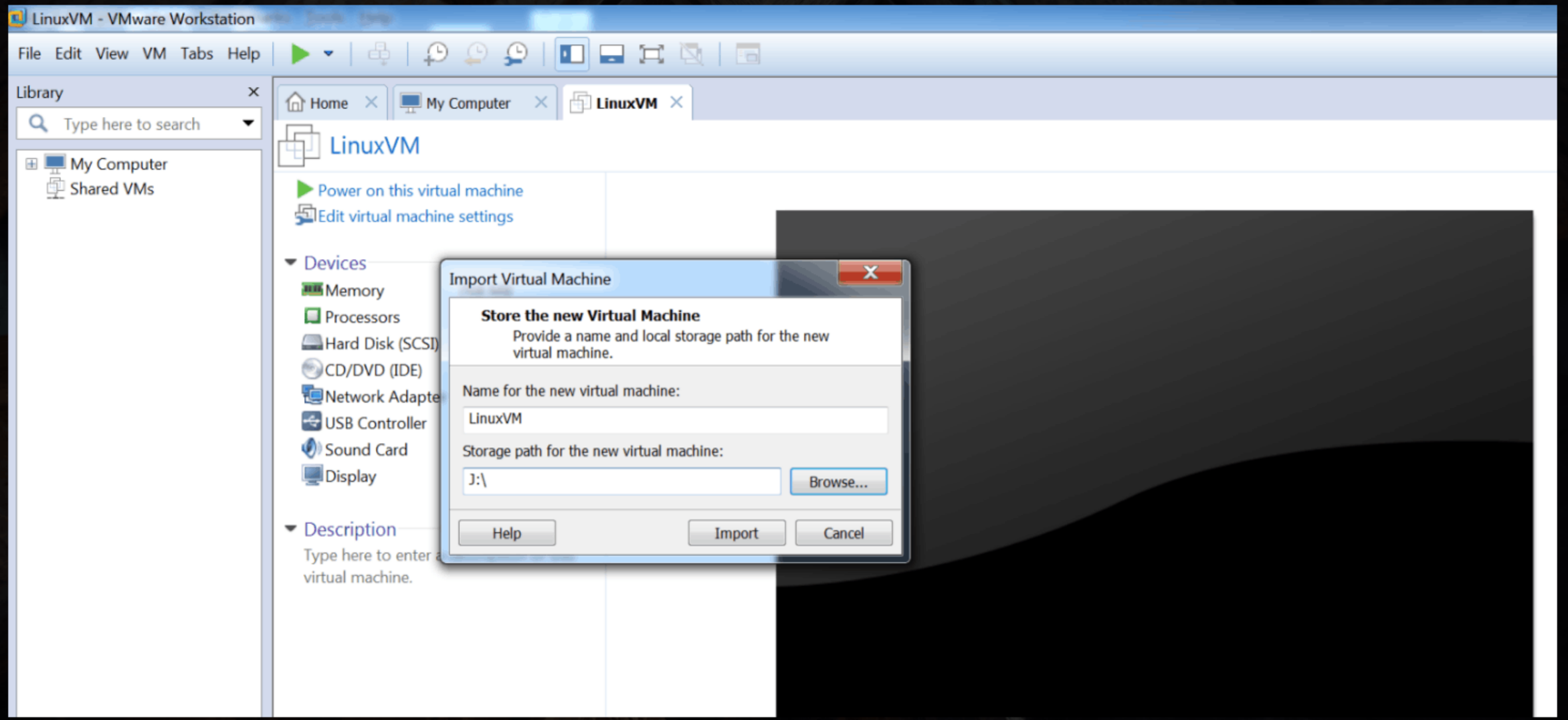


Configuring & Setting up Linux VM

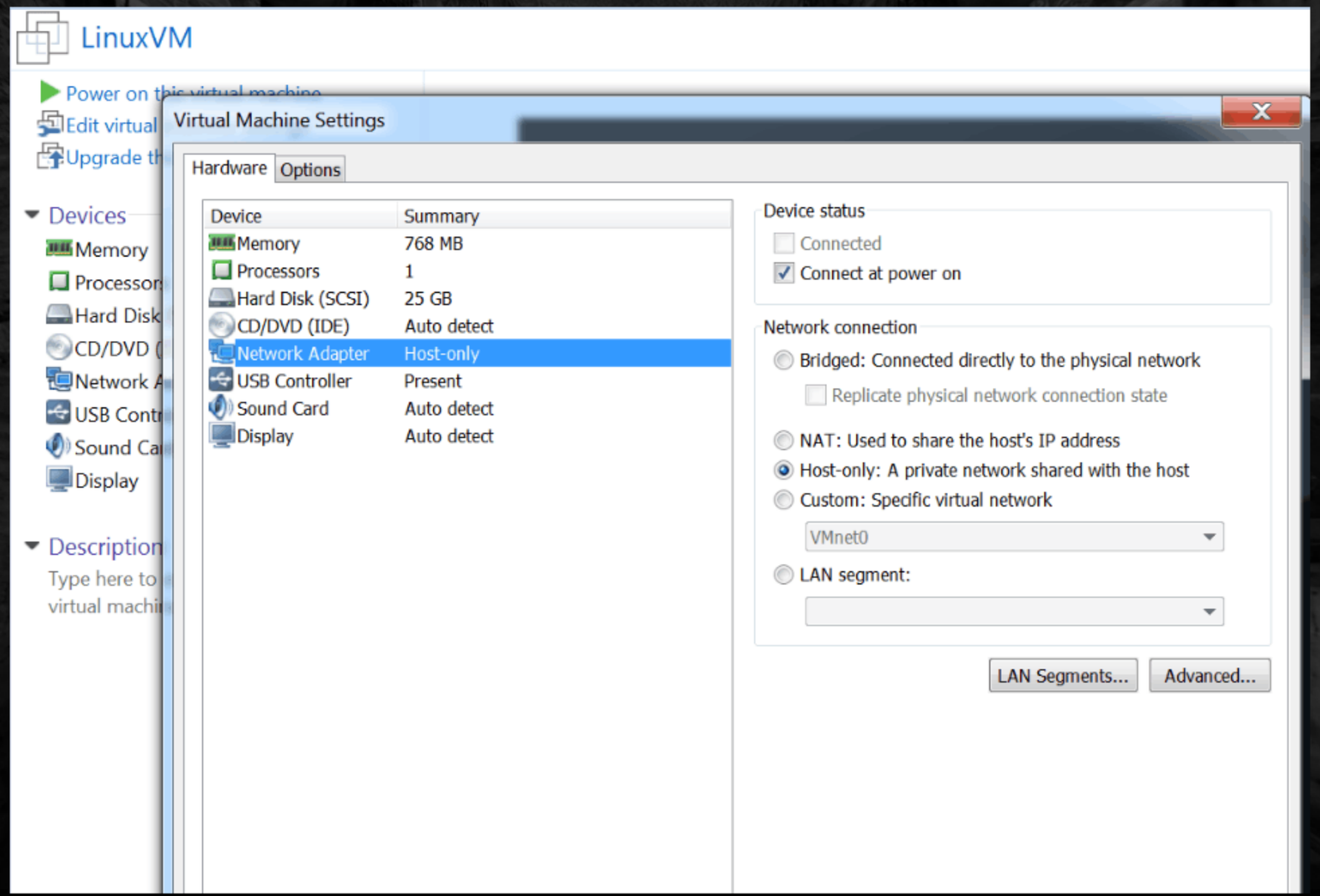
Unzip the provided Linux VM, open the LinuxVM.ovf in VMware Workstation/Fusion



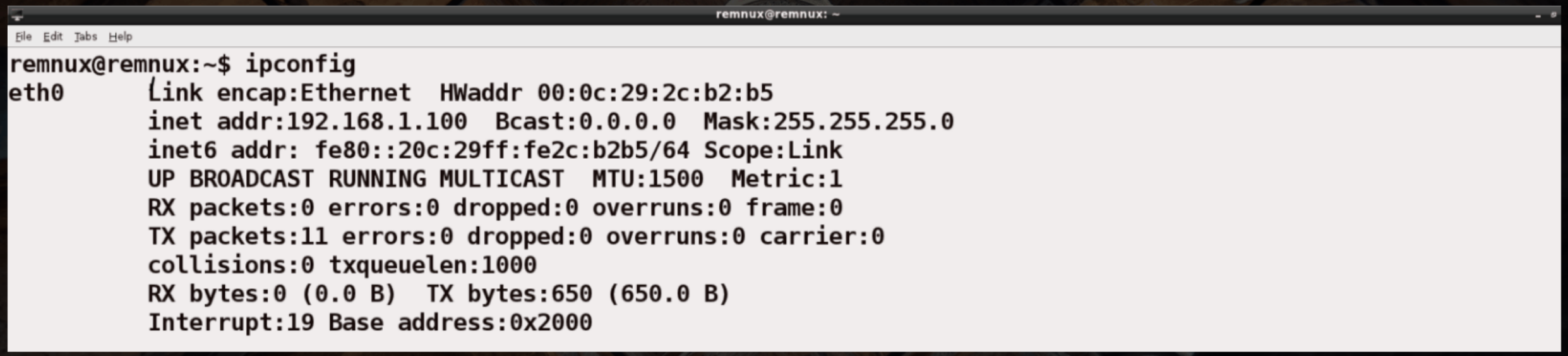
Provide the path to install the Linux VM and click on ***import***



The Linux VM is configured to run in host only mode

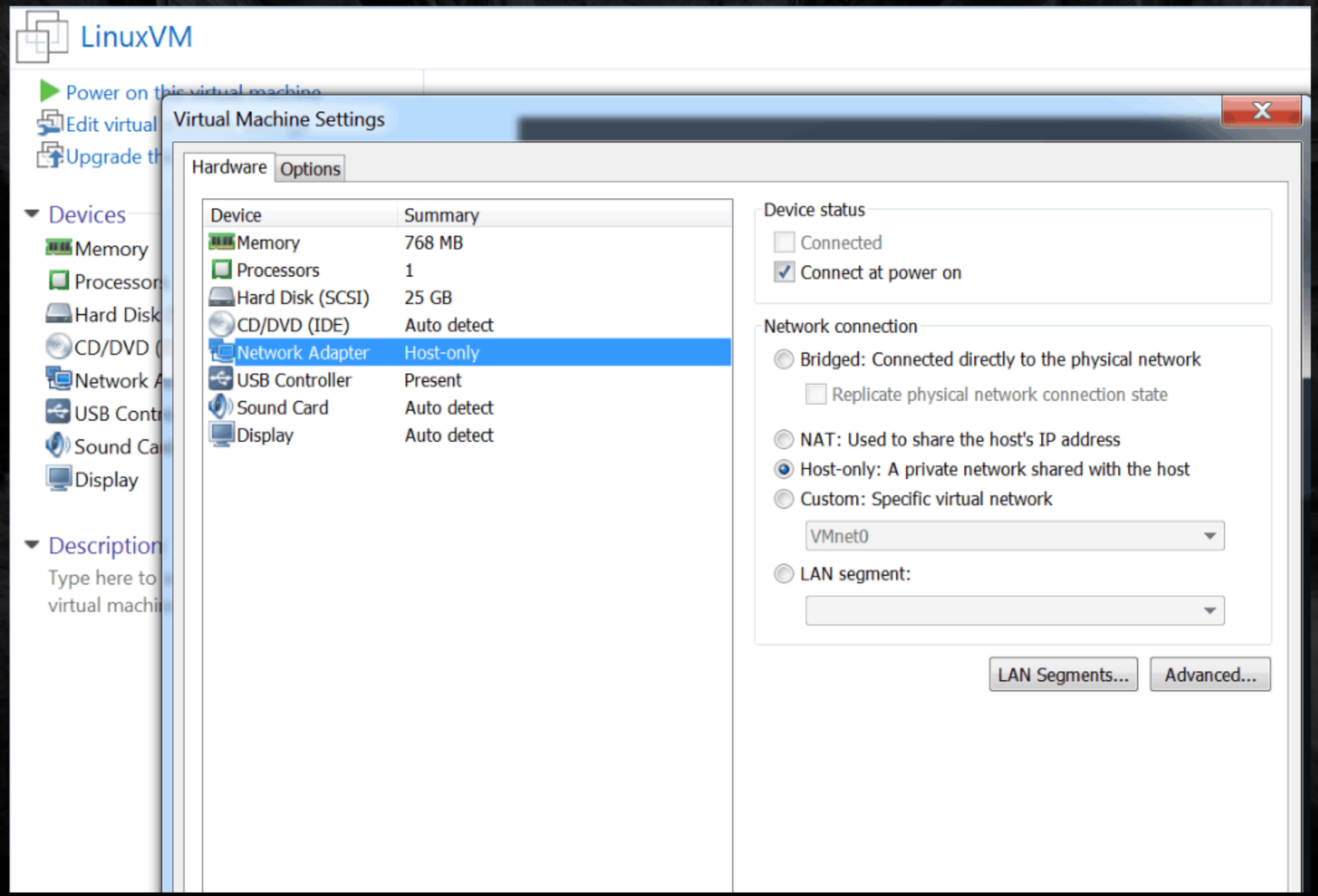


IP address of Linux VM is pre-configured to 192.168.1.100

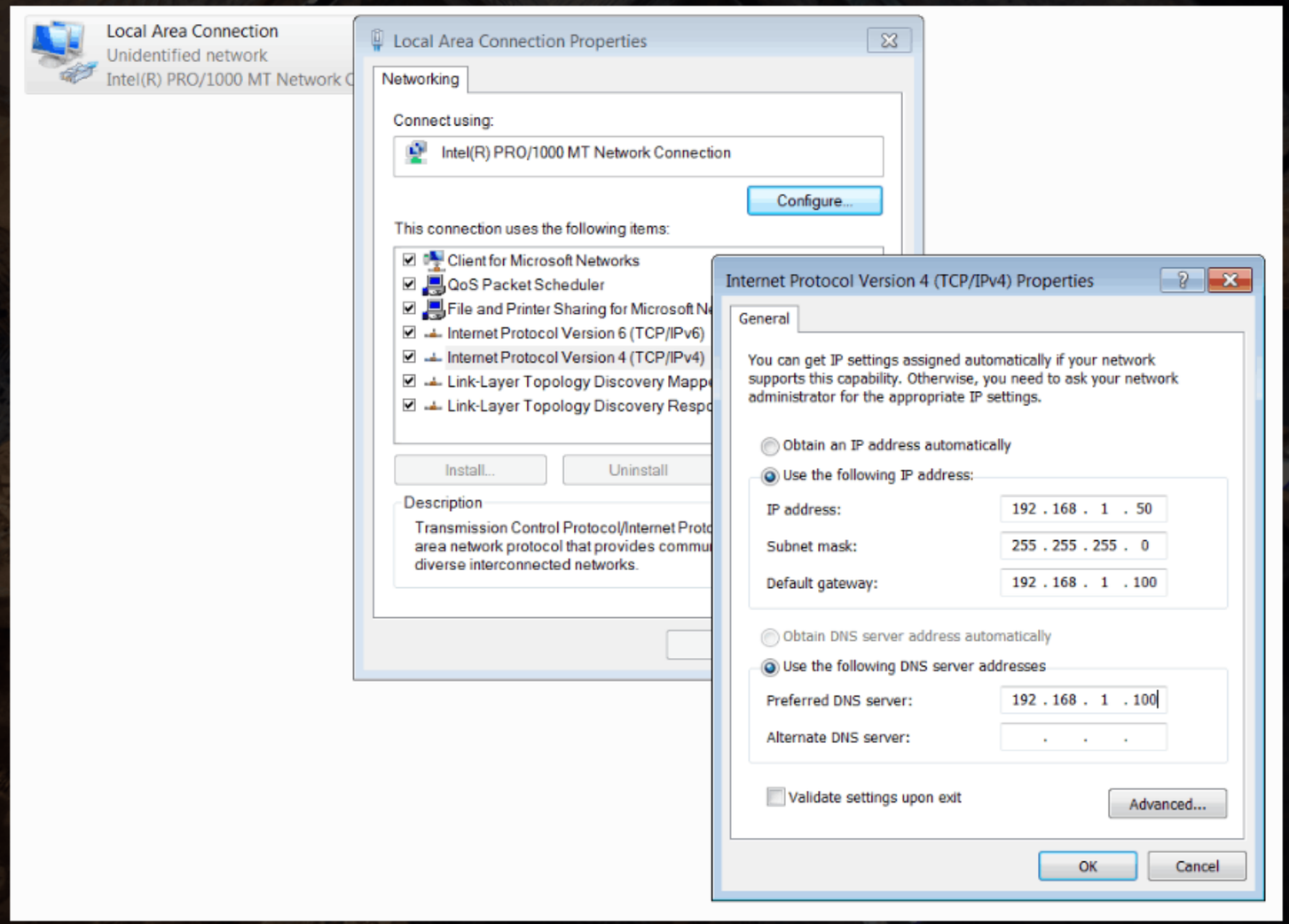


Configuring Windows VM

Configure the Windows VM to run in ***host-only*** mode



Configure the ***IP address*** and set the ***gateway*** and ***DNS*** to the Linux VM IP



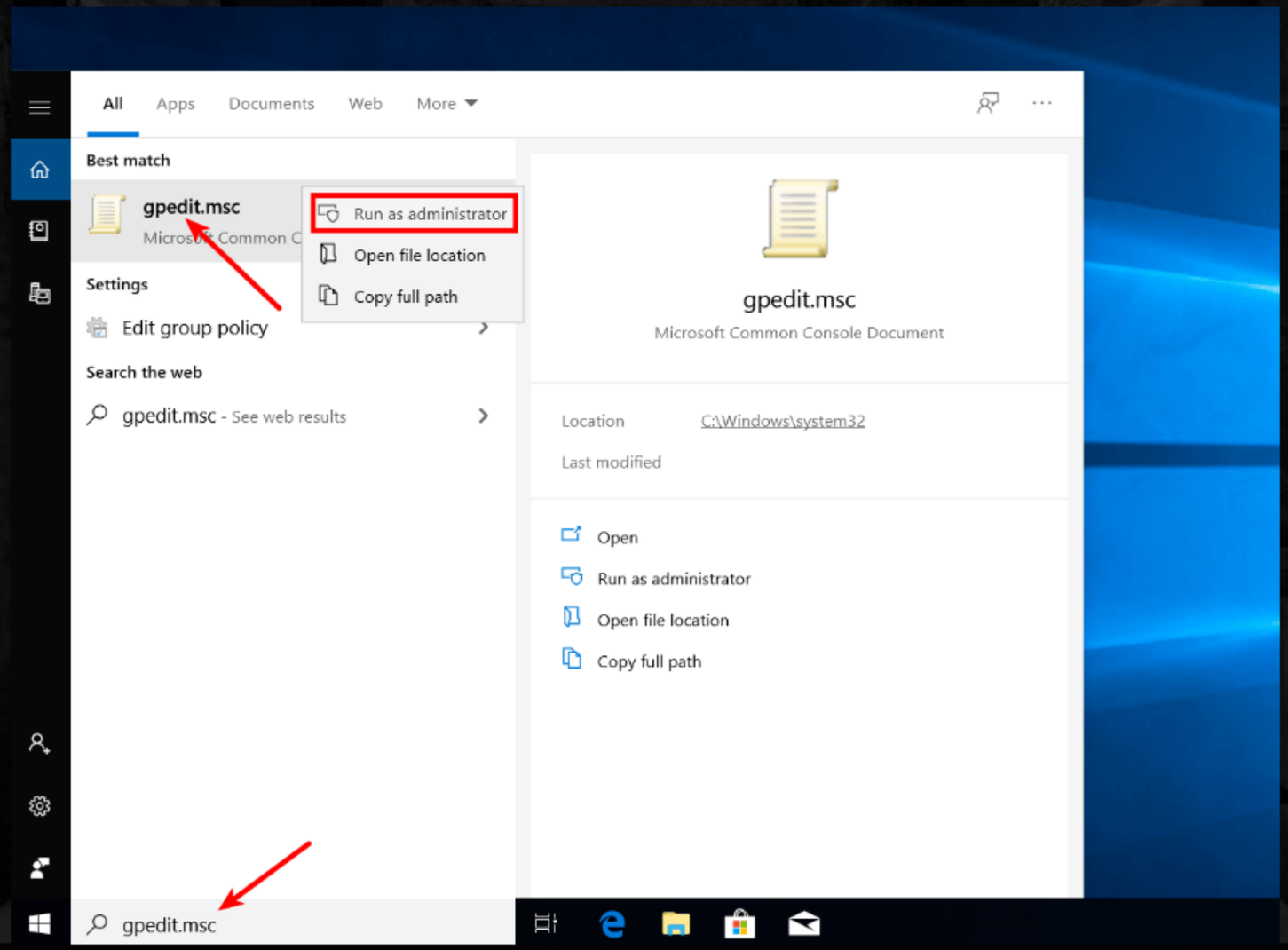
Check the connectivity between Windows and Linux VM

C:\Windows\system32\cmd.exe

```
C:\Users\training>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\training>
```

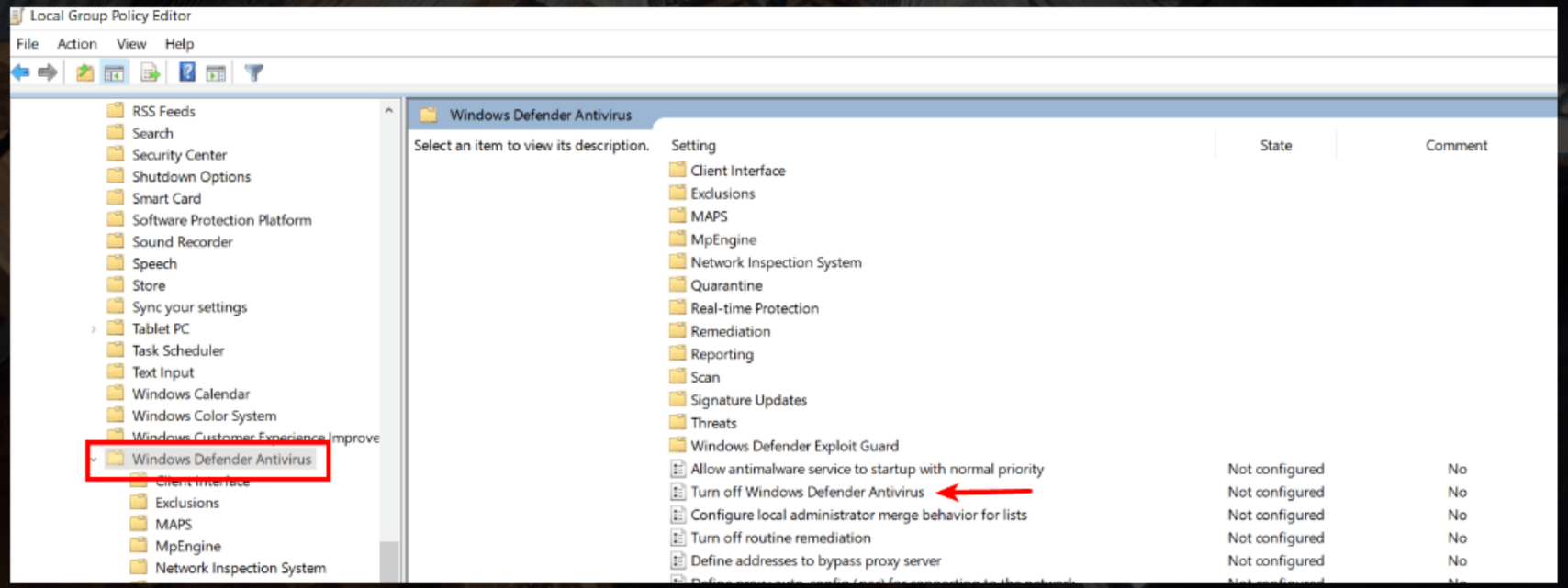
Disabling Windows Defender Service

Open the Local Group Policy Editor (*gpedit.msc*)

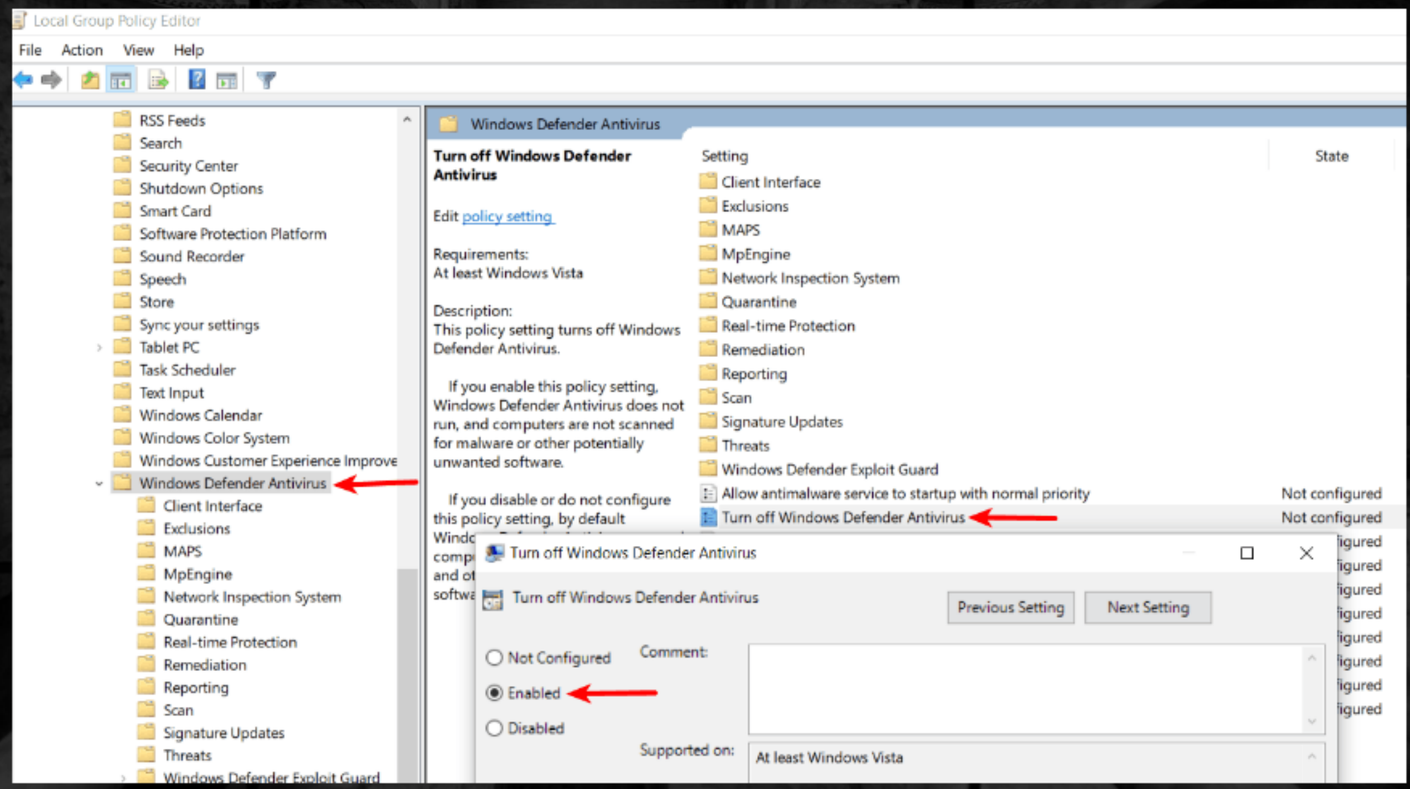


In the left pane of Local Group Policy Editor, navigate to the location below:

Computer Configuration\Administrative Templates\Windows Components\Windows Defender Antivirus



In the right pane of ***Windows Defender Antivirus*** in Local Group Policy Editor, double click/tap on the Turn off ***Windows Defender Antivirus*** policy to edit it then select ***Enabled*** and click on ***OK***



Take a clean snapshot on both Linux and Windows systems, so that you can revert back to a pristine state