

# **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



**Static  
Analysis**

**Analysis without  
executing the  
malware**



**Dynamic  
Analysis**

**Analysis by  
executing the  
malware**



**Memory  
Analysis**

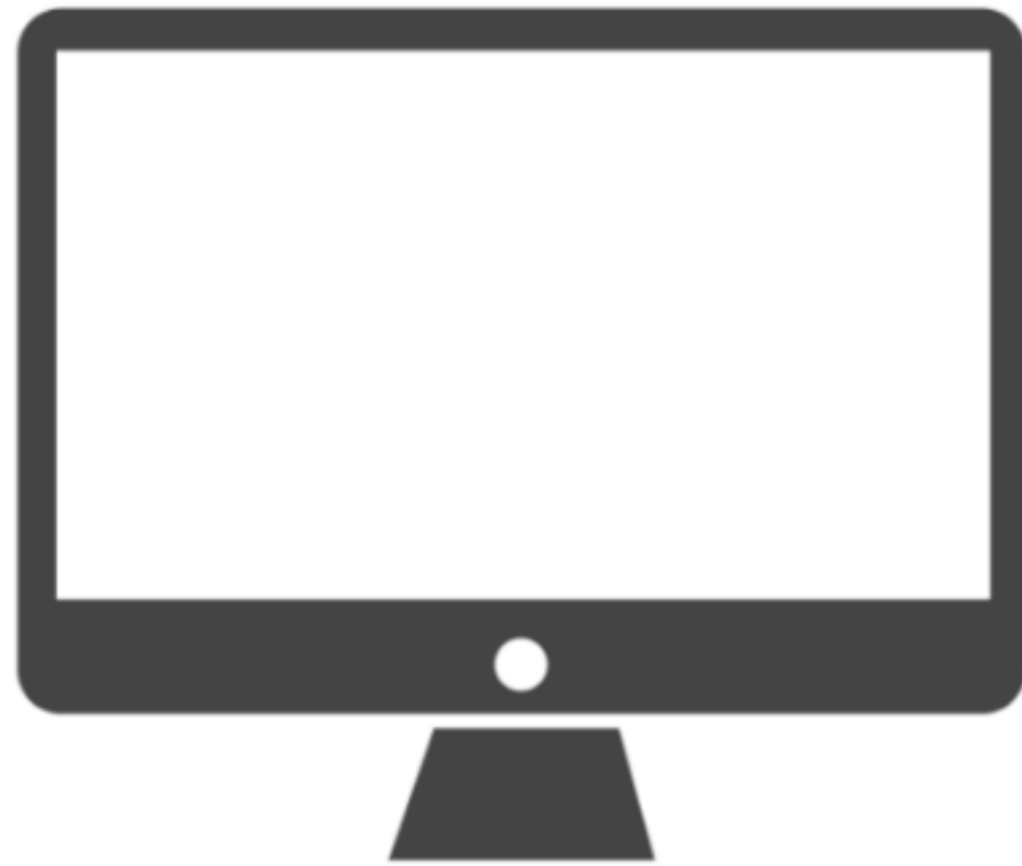
**Analysis of RAM (main  
memory) after  
executing the malware**



# Setting up the Lab Environment

# Lab Architecture

**Linux VM**



**IP: 192.168.1.100**

**Windows VM**



**IP: 192.168.1.x**  
**Gw: 192.168.1.100**  
**Dns: 192.168.1.100**

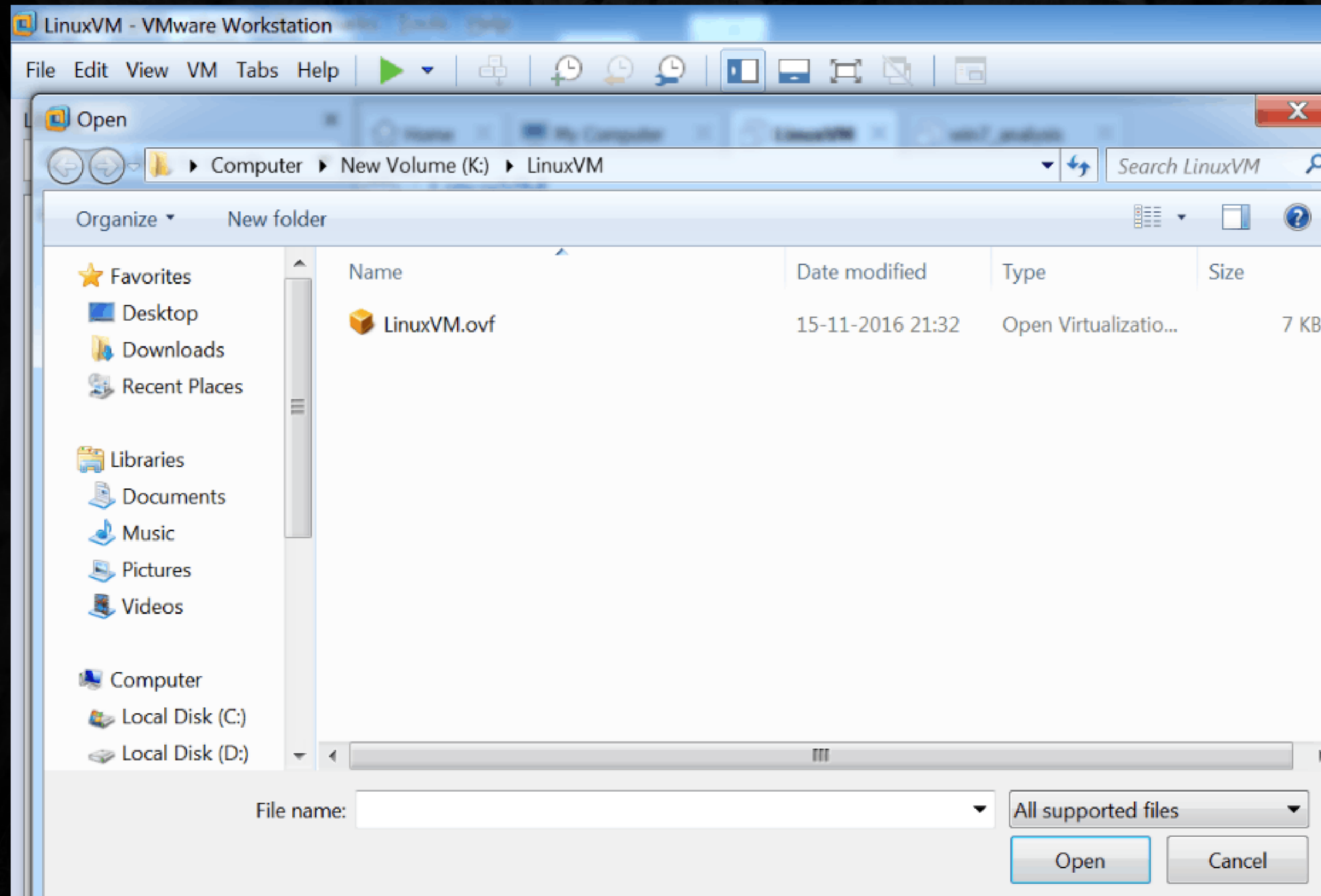


**Both Linux &  
windows VM  
running in host  
mode**

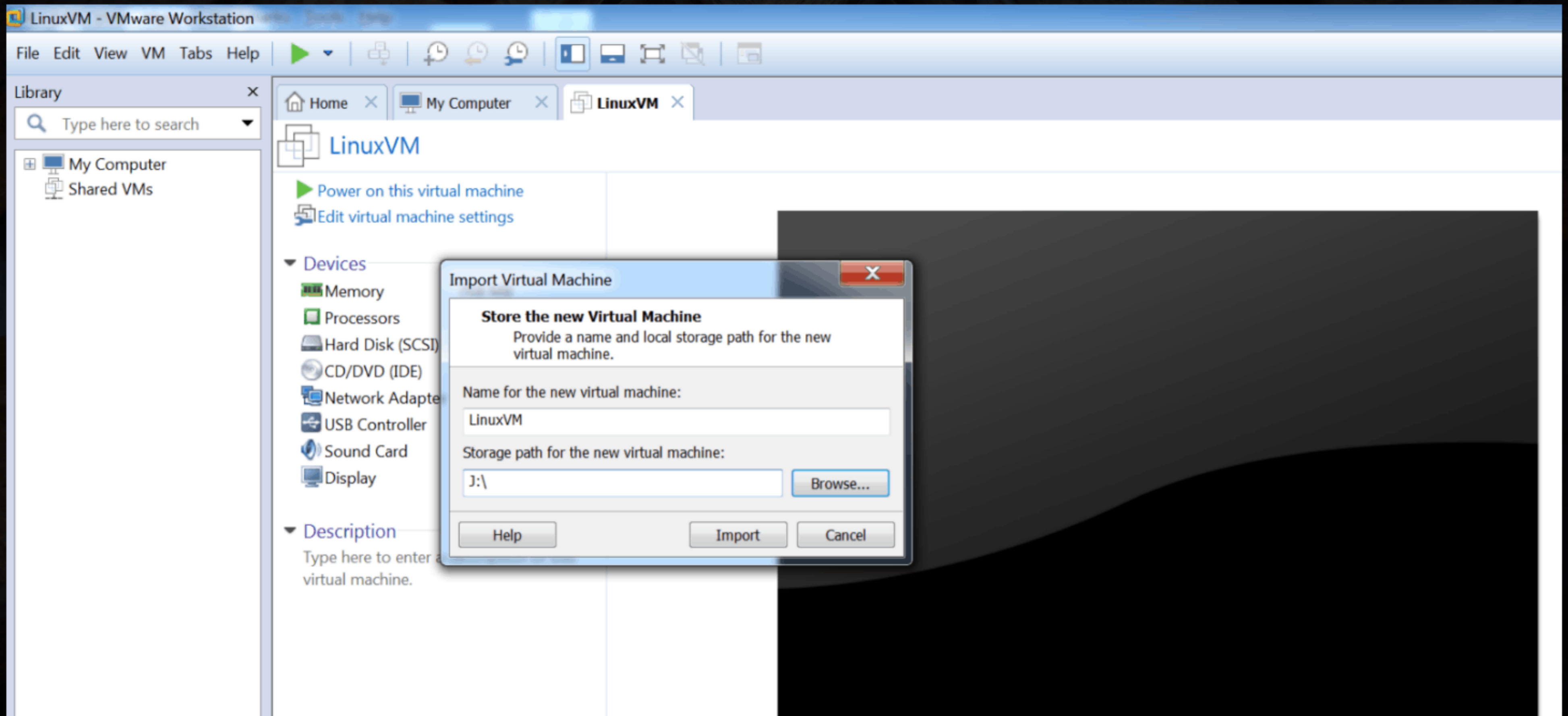


# **Configuring & Setting up Linux VM**

# 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

The screenshot shows the 'Virtual Machine Settings' dialog box for a Linux VM. The 'Options' tab is selected, and the 'Network Adapter' device is highlighted in the hardware list. The 'Device status' section shows 'Connect at power on' is checked. The 'Network connection' section shows 'Host-only' is selected as the network connection type, with 'VMnet0' selected in the dropdown menu. The 'LAN segment' dropdown is empty. There are buttons for 'LAN Segments...' and 'Advanced...' at the bottom right.

Device	Summary
Memory	768 MB
Processors	1
Hard Disk (SCSI)	25 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

- Connected
- Connect at power on

Network connection

- Bridged: Connected directly to the physical network
  - Replicate physical network connection state
- NAT: Used to share the host's IP address
- Host-only: A private network shared with the host
- Custom: Specific virtual network

VMnet0

LAN segment:

LAN Segments... Advanced...

# IP address of Linux VM is pre-configured to 192.168.1.100

```
remnux@remnux: ~  
File Edit Tabs Help  
remnux@remnux:~$ ipconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2c:b2:b5  
          inet addr:192.168.1.100  Bcast:0.0.0.0  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe2c:b2b5/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:650 (650.0 B)  
          Interrupt:19 Base address:0x2000
```



# Configuring Windows VM

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

The screenshot shows the LinuxVM application window with the 'Virtual Machine Settings' dialog box open. The 'Options' tab is selected, and the 'Network Adapter' is highlighted in the device list. The 'Host-only' radio button is selected under the 'Network connection' section.

**Virtual Machine Settings**

Hardware Options

Device	Summary
Memory	768 MB
Processors	1
Hard Disk (SCSI)	25 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

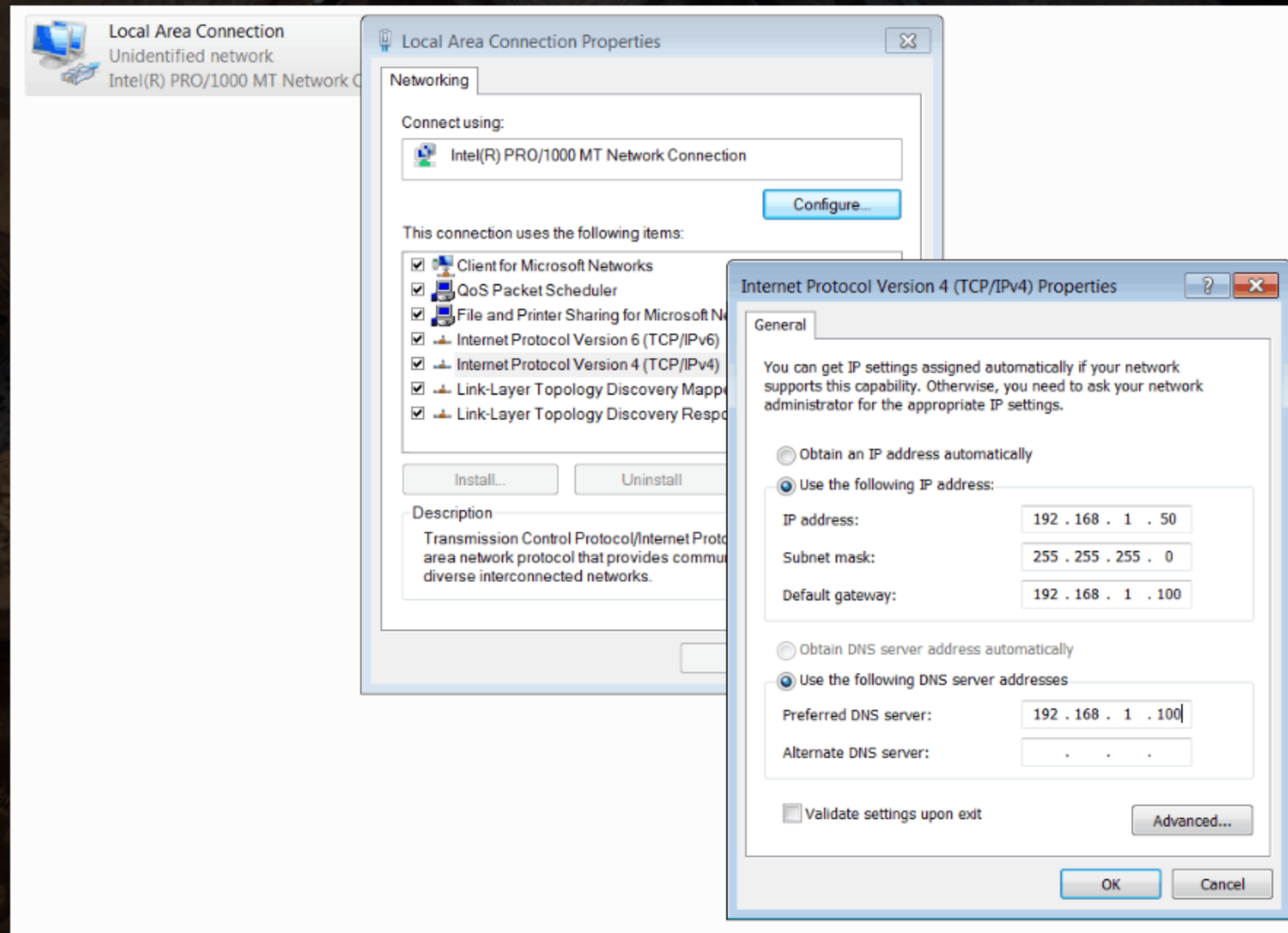
- Connected
- Connect at power on

Network connection

- Bridged: Connected directly to the physical network
  - Replicate physical network connection state
- NAT: Used to share the host's IP address
- Host-only: A private network shared with the host
- Custom: Specific virtual network
  - VMnet0
- LAN segment:
  -

LAN Segments... Advanced...

# 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:
```

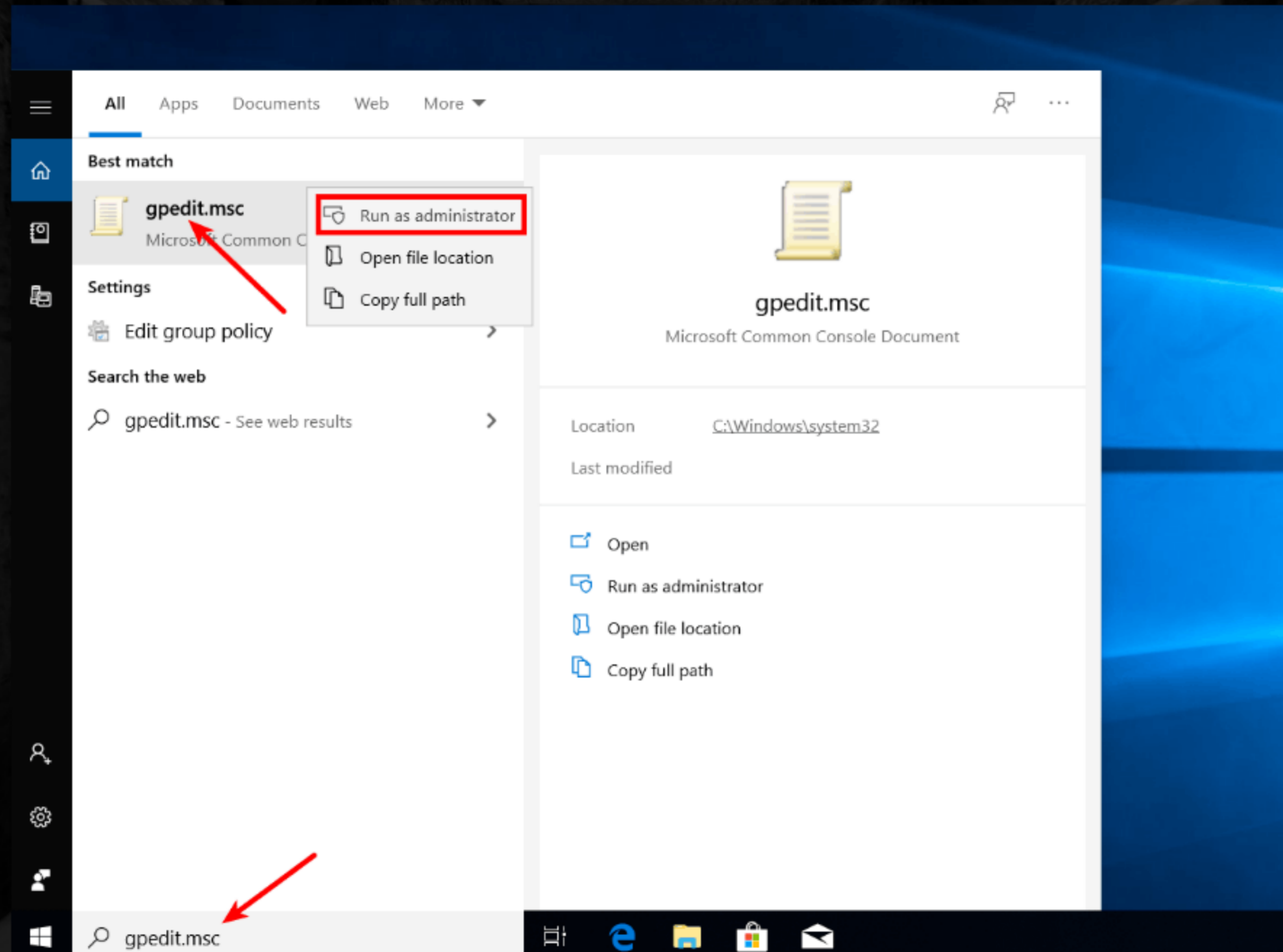
```
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\Users\training>
```



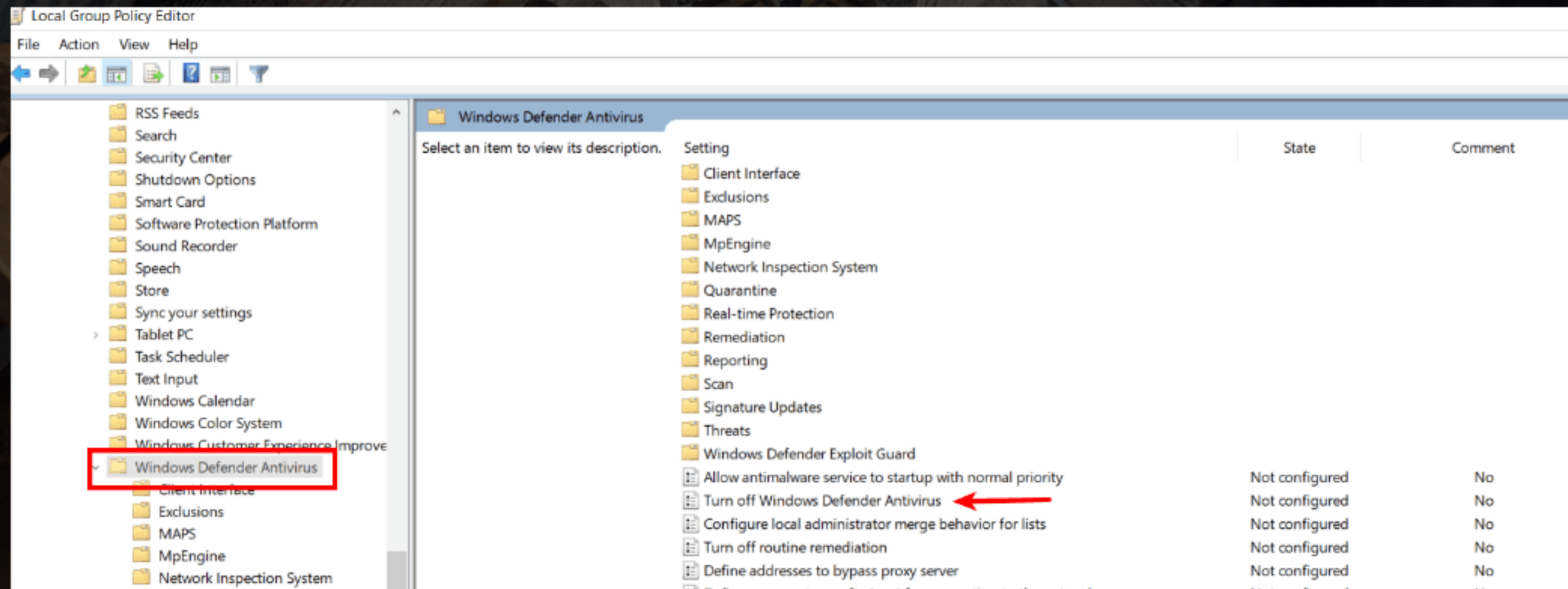
# **Disabling Windows Defender Service**

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

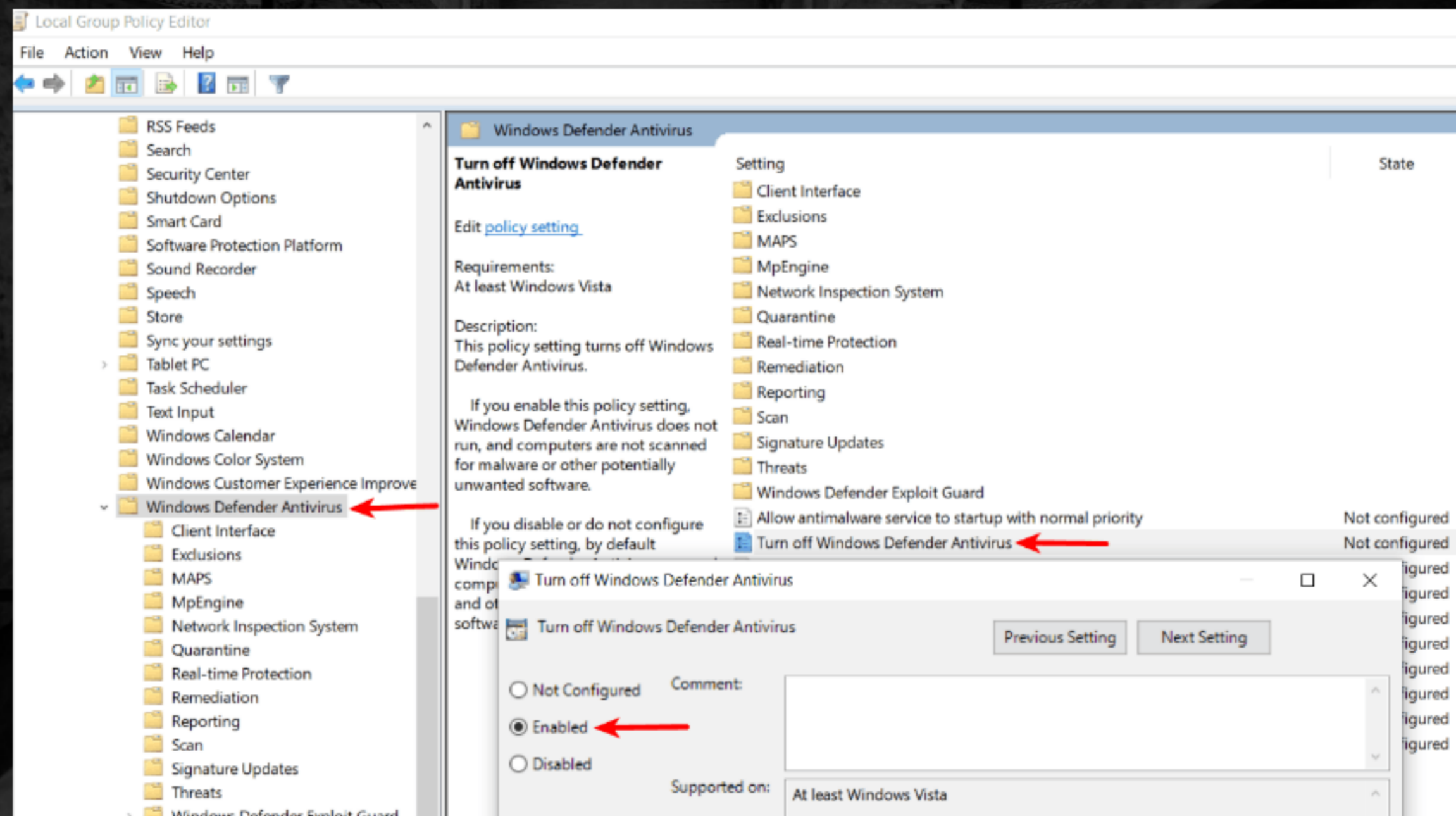


**In the left pane of Local Group Policy Editor, navigate to the location below:**

***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

