

Advanced Web Hacking

---

# OVA Import & VPN Setup Guide





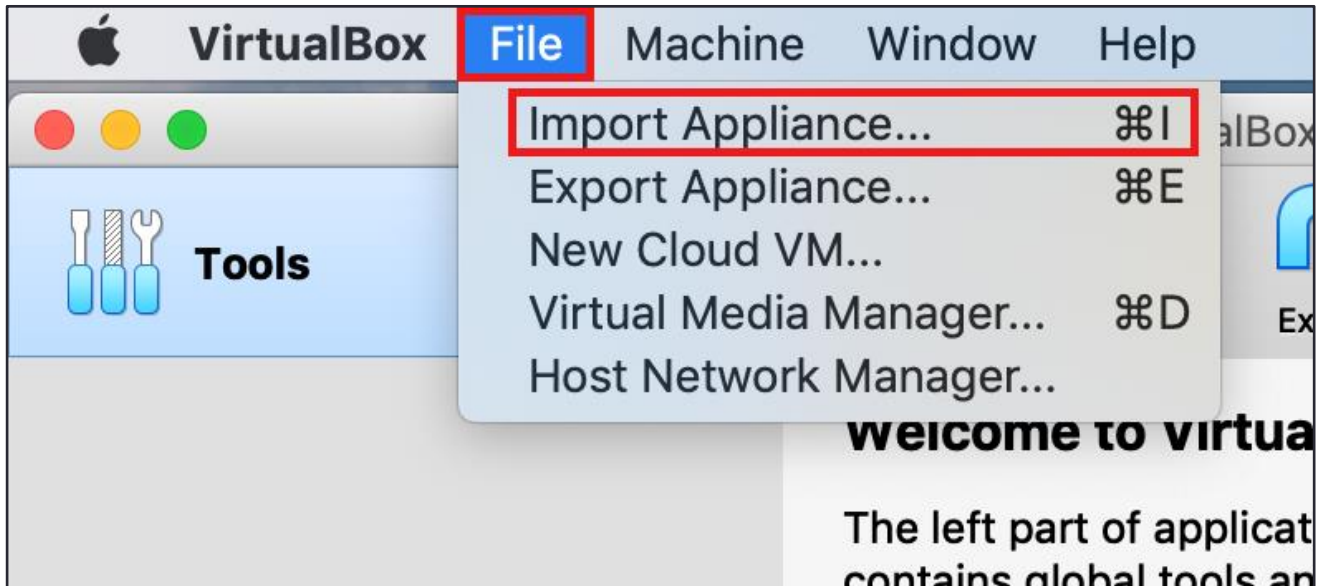
# Contents

<b>OVA Import</b> .....	<b>2</b>
For VirtualBox on Mac.....	2
For VirtualBox on Windows .....	5
For VirtualBox on Linux.....	8
<b>VPN Setup</b> .....	<b>11</b>

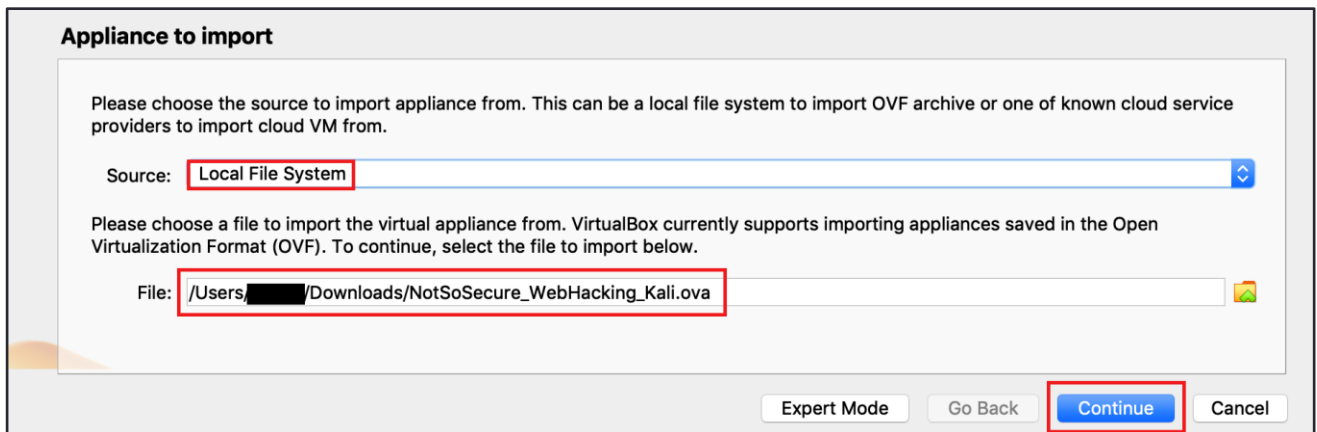
# OVA Import

## For VirtualBox on Mac

**Step 1:** Import the ova file in virtual box, Click on File → Import Appliance.



**Step 2:** Browse to the downloaded ova file 'NotSoSecure\_Web\_Hacking\_Training\_2020.ova' and click Continue.



**Step 3:** Review the settings and Check MAC Address Policy is set to 'Generate new MAC addresses for all network adapters' and click Import.

### Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
	Name: NotSoSecure_WebHacking_Kali
	Product: NotSoSecure Web Hacking Custom Kali
	Product-URL: https://notsosecure.com/hacking-training/advanced-web-hacking/
	Vendor: NotSoSecure Global Services, A Claranet Group Company
	Vendor-URL: https://notsosecure.com/
	Version: 2021v1
	Description: Welcome to Advanced Web Hacking/ Web Hacking Black Belt Edition Training. ...
	Guest OS Type:  Ubuntu (64-bit)
	CPU: 3
	RAM: 4096 MB
	DVD: <input checked="" type="checkbox"/>
	USB Controller: <input checked="" type="checkbox"/>
	Sound Card: <input checked="" type="checkbox"/> ICH AC97
	Network Adapter: <input checked="" type="checkbox"/> Intel PRO/1000 MT Desktop (82540EM)
	Storage Controller (IDE): PIIX4
	Storage Controller (IDE): PIIX4
	Storage Controller (SATA): AHCI
	Virtual Disk Image: NotSoSecure_WebHacking_Kali-disk001.vmdk
	Base Folder: /Users/[redacted]/VirtualBox VMs
	Primary Group: /

Machine Base Folder:

MAC Address Policy: Generate new MAC addresses for all network adapters

Additional Options:  Import hard drives as VDI

Appliance is not signed

Restore Defaults Go Back Import Cancel

**Step 4:** Installation of the VM progresses.

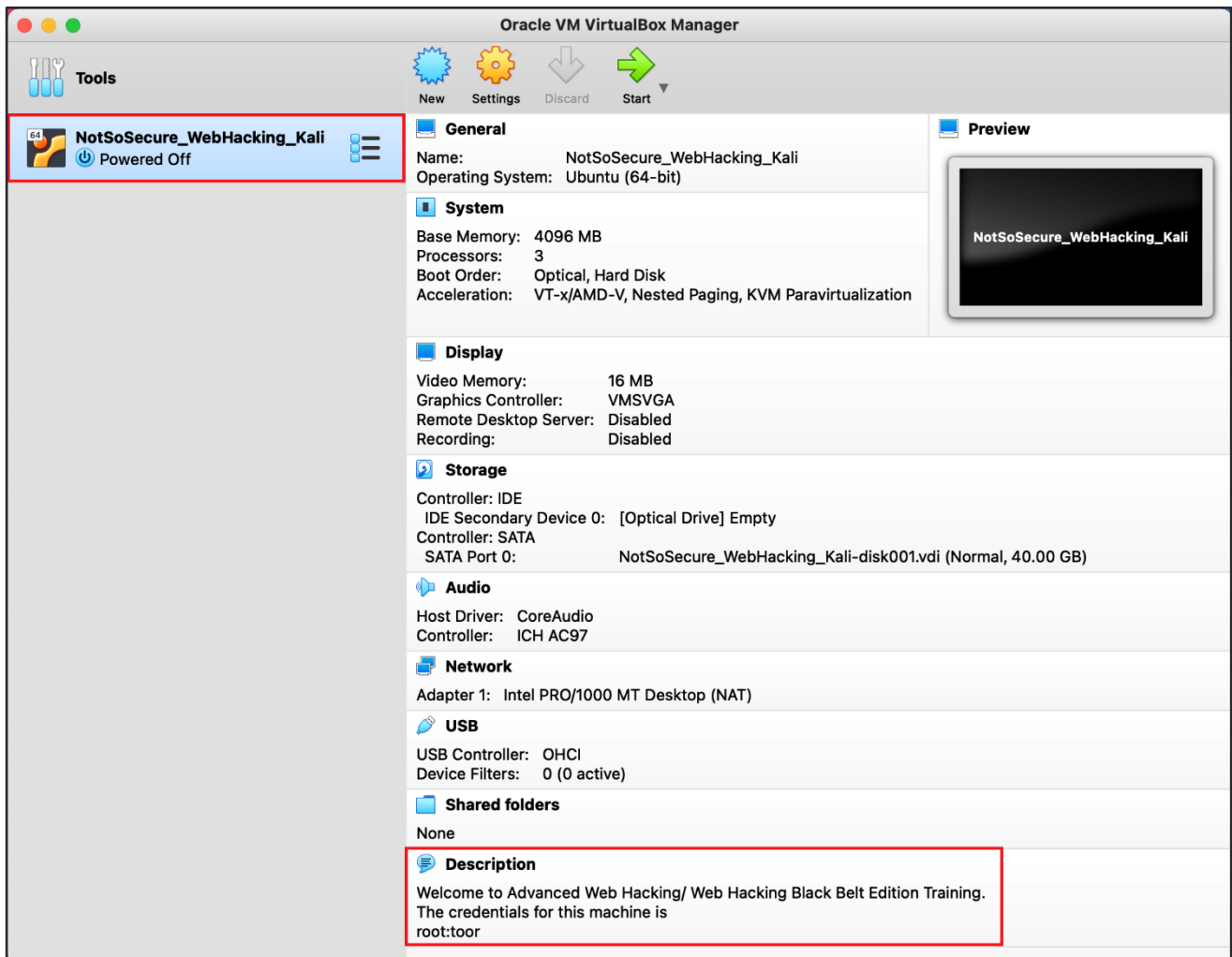
Importing virtual disk image 'NotSoSecure\_WebHacking\_Kali-disk001.vmdk' ... (2/3)

1 minute, 42 seconds remaining

✕

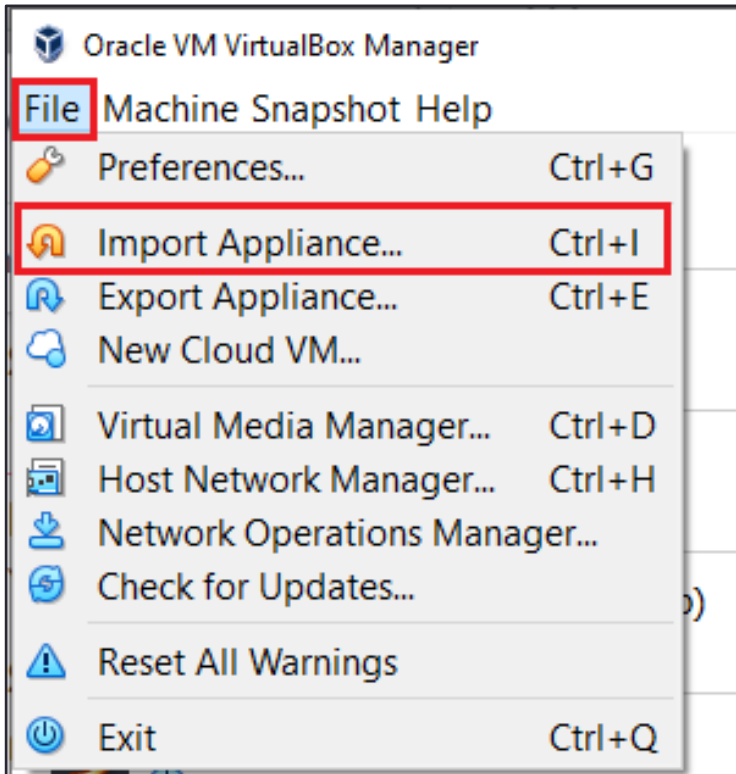
**Step 5:** Import has been successful; the machine credentials are highlighted in the image. Start the VM and use the credentials mentioned for the login.

- **Username:** root
- **Password:** toor

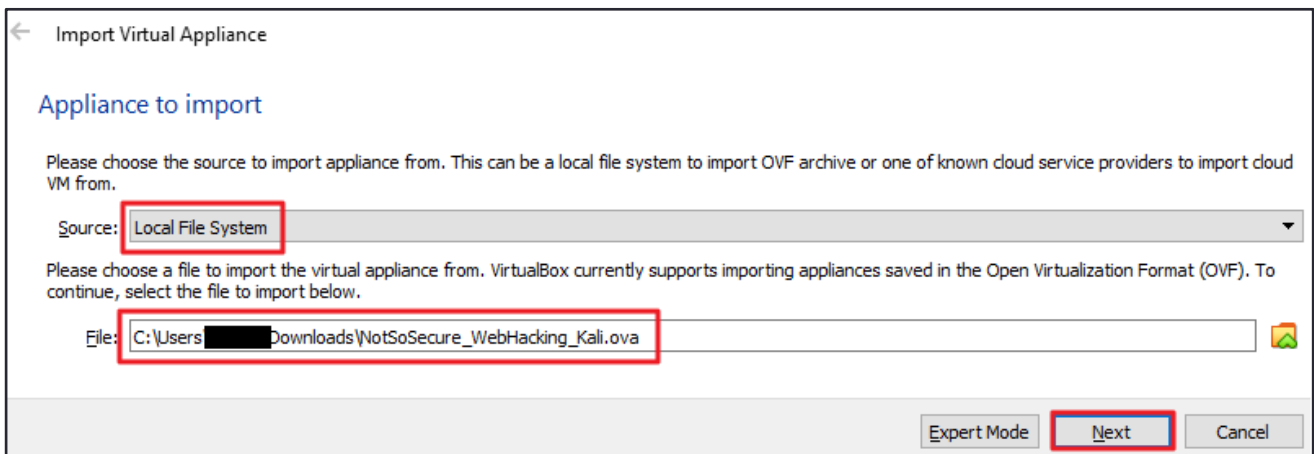


# For VirtualBox on Windows

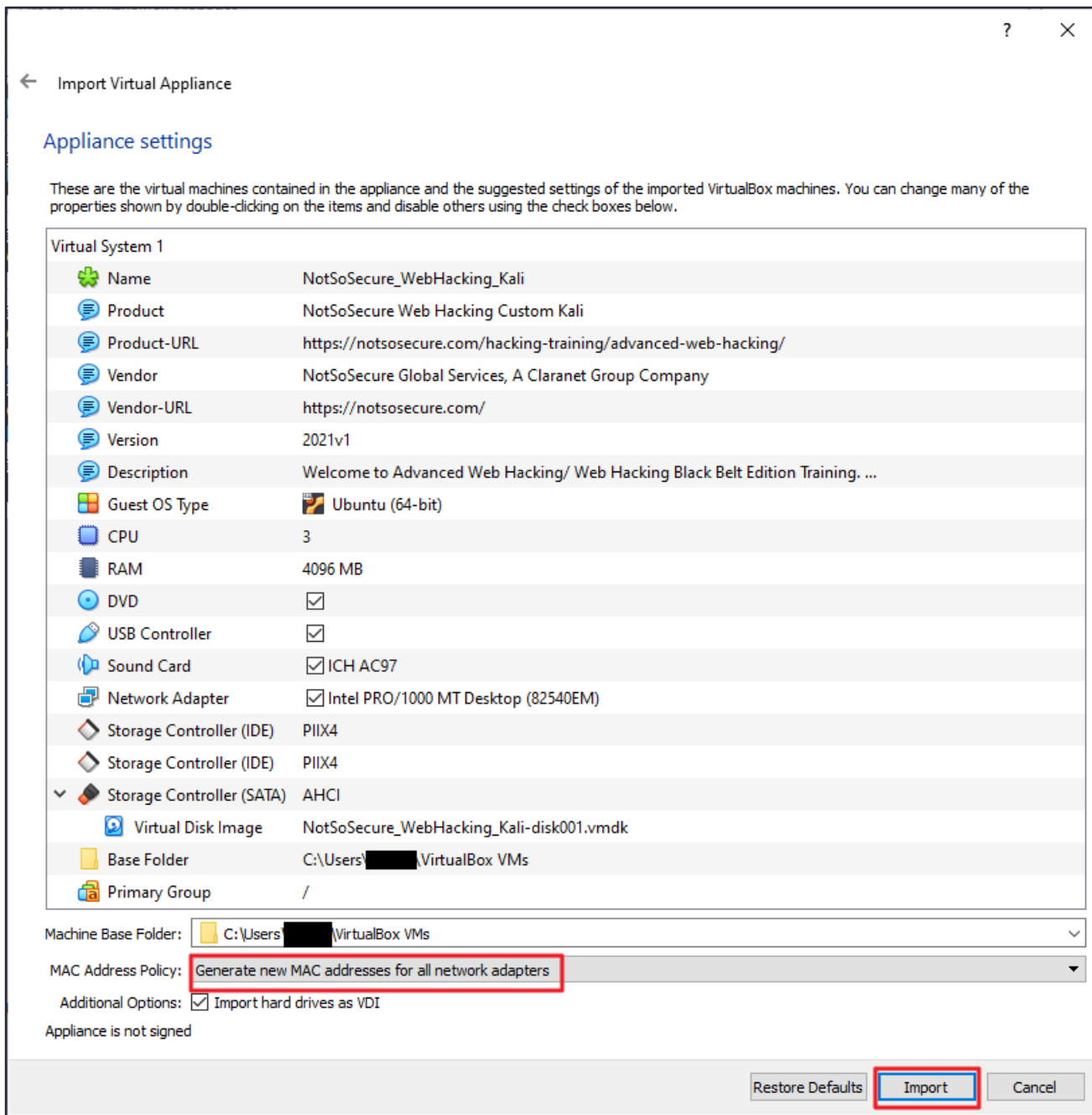
**Step 1:** Import the ova file in virtual box, Click on File → Import Appliance.



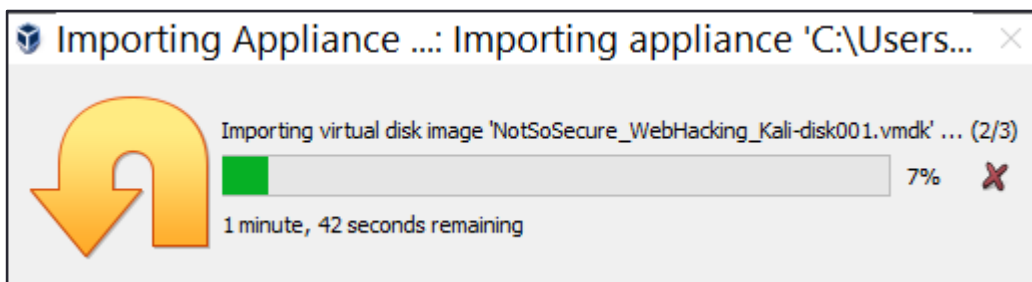
**Step 2:** Browse to the downloaded ova file 'NotSoSecure\_Web\_Hacking\_Training\_2020.ova' and click Continue.



**Step 3:** Review the settings and Check MAC Address Policy is set to 'Generate new MAC addresses for all network adapters' and click Import.

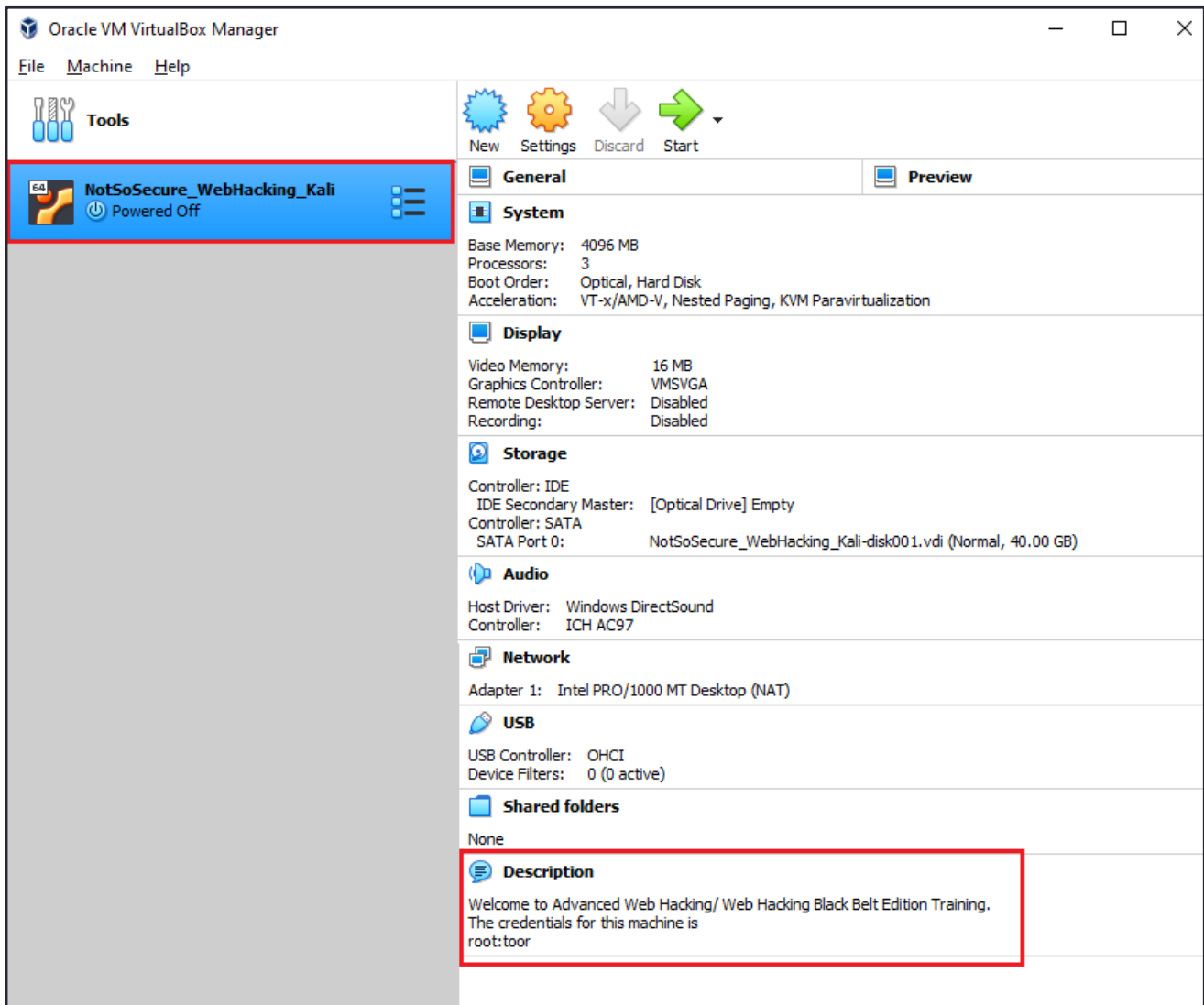


**Step 4:** Installation of the VM progresses.



**Step 5:** Import has been successful; the machine credentials are highlighted in the image. Start the VM and use the credentials mentioned for the login.

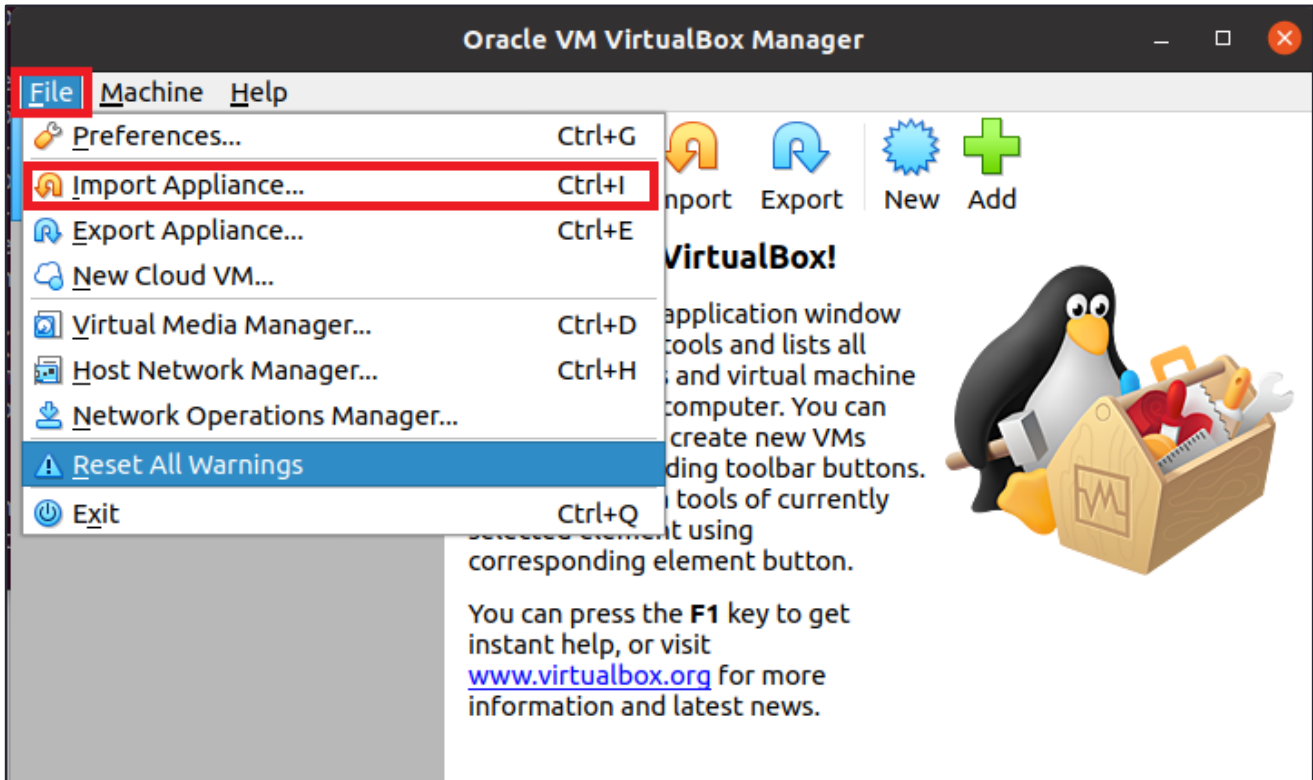
- **Username:** root
- **Password:** toor



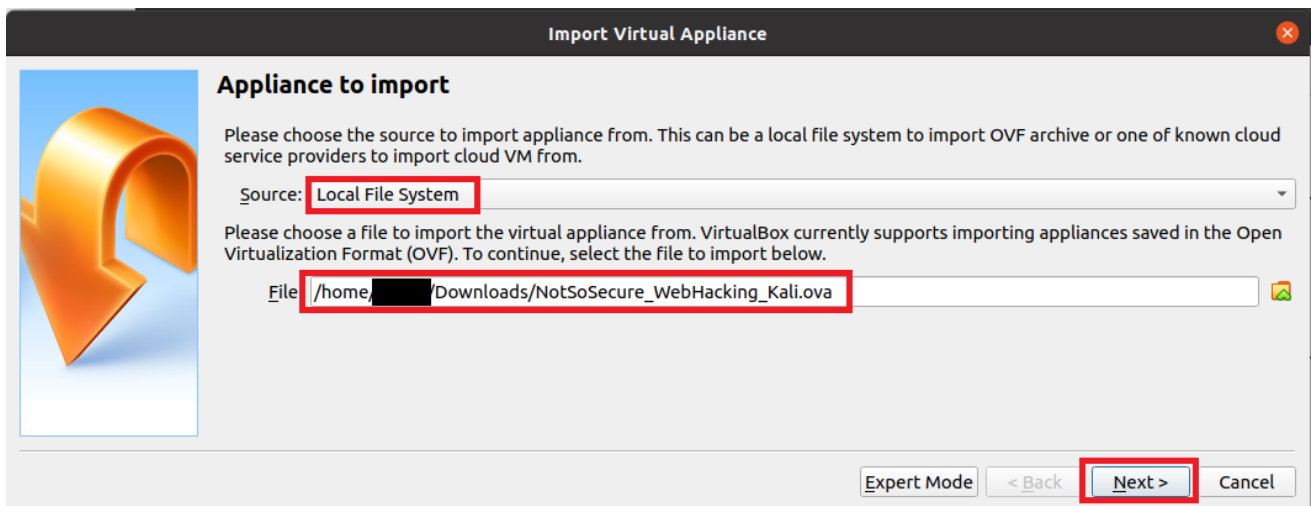


# For VirtualBox on Linux

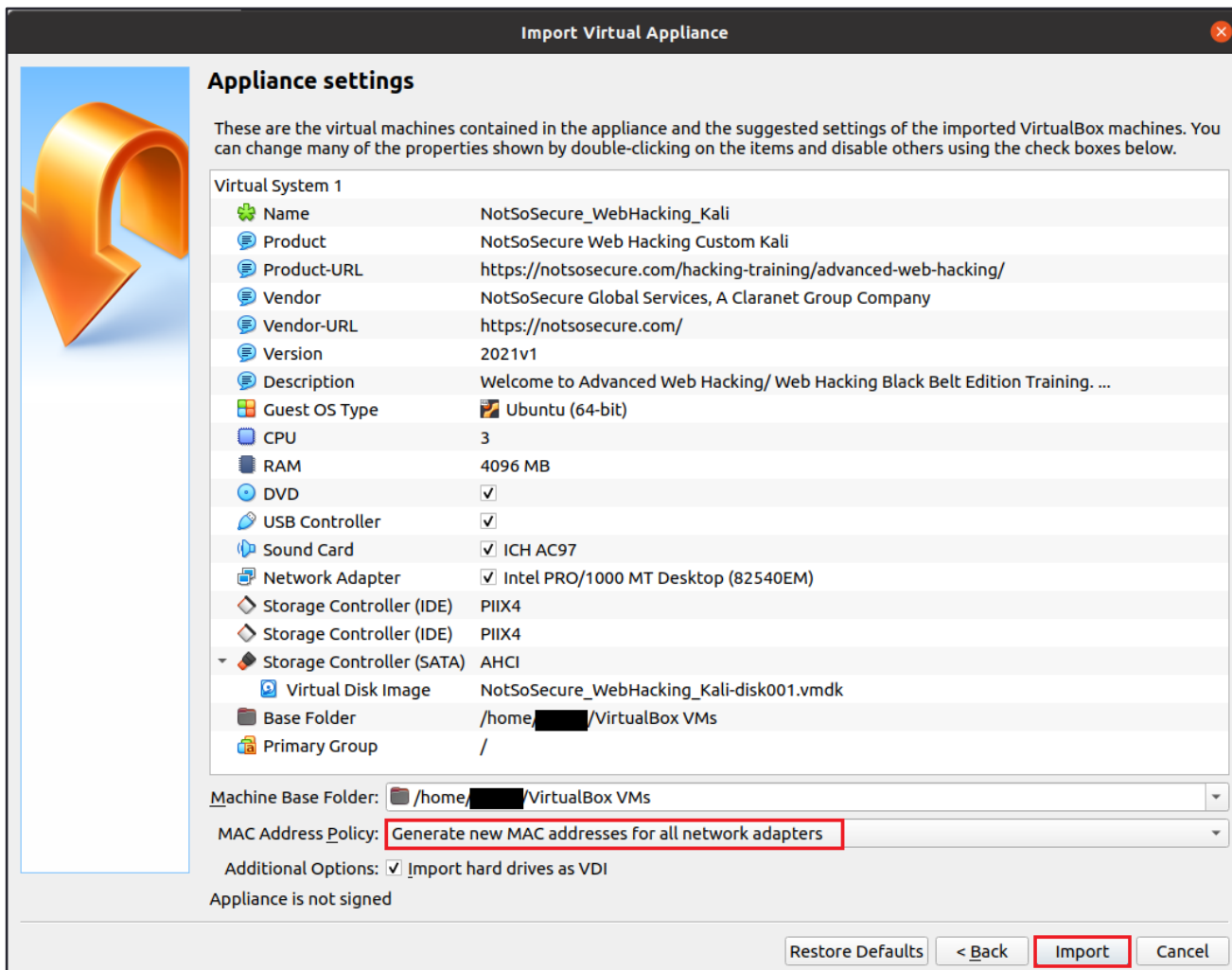
**Step 1:** Import the ova file in virtual box, Click on File → Import Appliance.



**Step 2:** Browse to the downloaded ova file 'NotSoSecure\_Web\_Hacking\_Training\_2020.ova' and click Continue.



**Step 3:** Review the settings and Check MAC Address Policy is set to 'Generate new MAC addresses for all network adapters' and click Import.



**Import Virtual Appliance**

**Appliance settings**

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	NotSoSecure_WebHacking_Kali
Product	NotSoSecure Web Hacking Custom Kali
Product-URL	https://notsosecure.com/hacking-training/advanced-web-hacking/
Vendor	NotSoSecure Global Services, A Claranet Group Company
Vendor-URL	https://notsosecure.com/
Version	2021v1
Description	Welcome to Advanced Web Hacking/ Web Hacking Black Belt Edition Training. ...
Guest OS Type	Ubuntu (64-bit)
CPU	3
RAM	4096 MB
DVD	<input checked="" type="checkbox"/>
USB Controller	<input checked="" type="checkbox"/>
Sound Card	<input checked="" type="checkbox"/> ICH AC97
Network Adapter	<input checked="" type="checkbox"/> Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)	PIIX4
Storage Controller (IDE)	PIIX4
Storage Controller (SATA)	AHCI
Virtual Disk Image	NotSoSecure_WebHacking_Kali-disk001.vmdk
Base Folder	/home/██████/VirtualBox VMs
Primary Group	/

Machine Base Folder: /home/██████/VirtualBox VMs

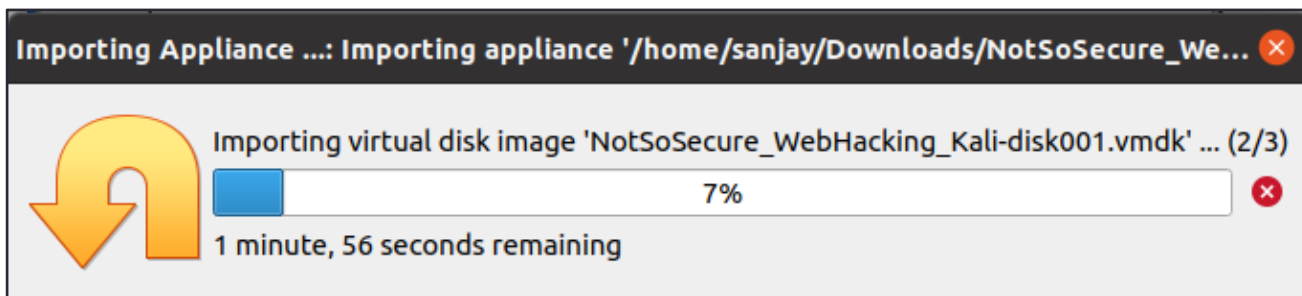
MAC Address Policy: **Generate new MAC addresses for all network adapters**

Additional Options:  Import hard drives as VDI

Appliance is not signed

Restore Defaults < Back **Import** Cancel

**Step 4:** Installation of the VM progresses.



**Importing Appliance ...: Importing appliance '/home/sanjay/Downloads/NotSoSecure\_We...**

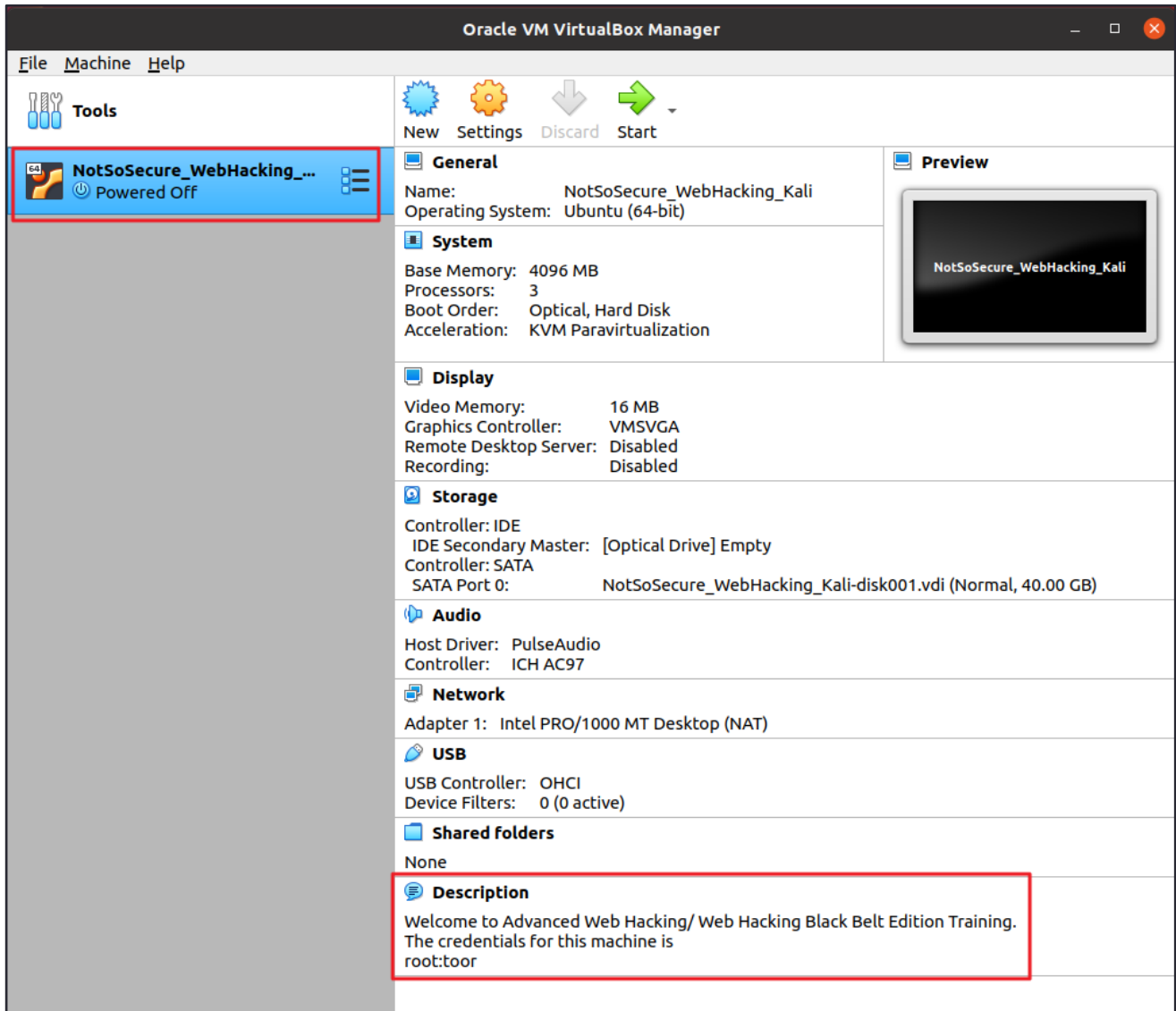
Importing virtual disk image 'NotSoSecure\_WebHacking\_Kali-disk001.vmdk' ... (2/3)

7%

1 minute, 56 seconds remaining

**Step 5:** Import has been successful; the machine credentials are highlighted in the image. Start the VM and use the credentials mentioned for the login.

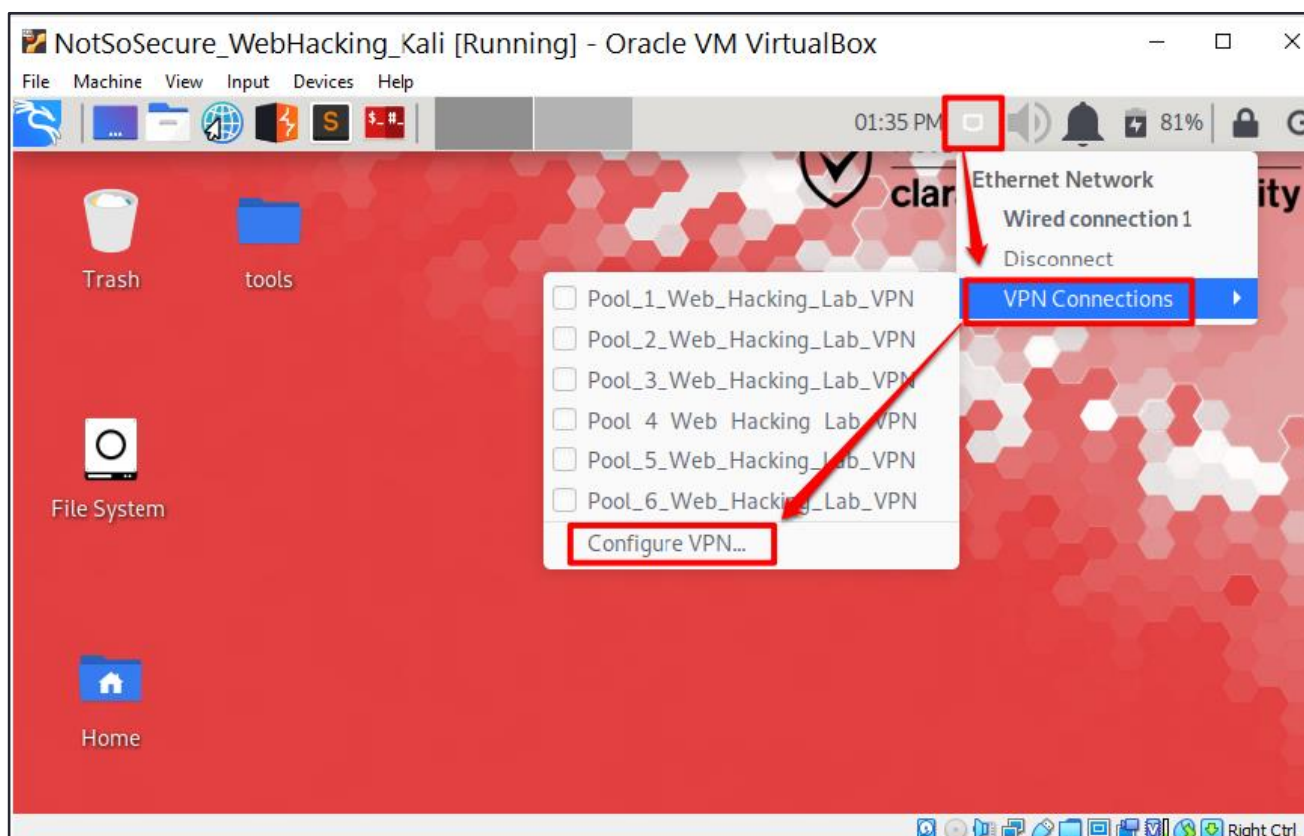
- **Username:** root
- **Password:** toor



# VPN Setup

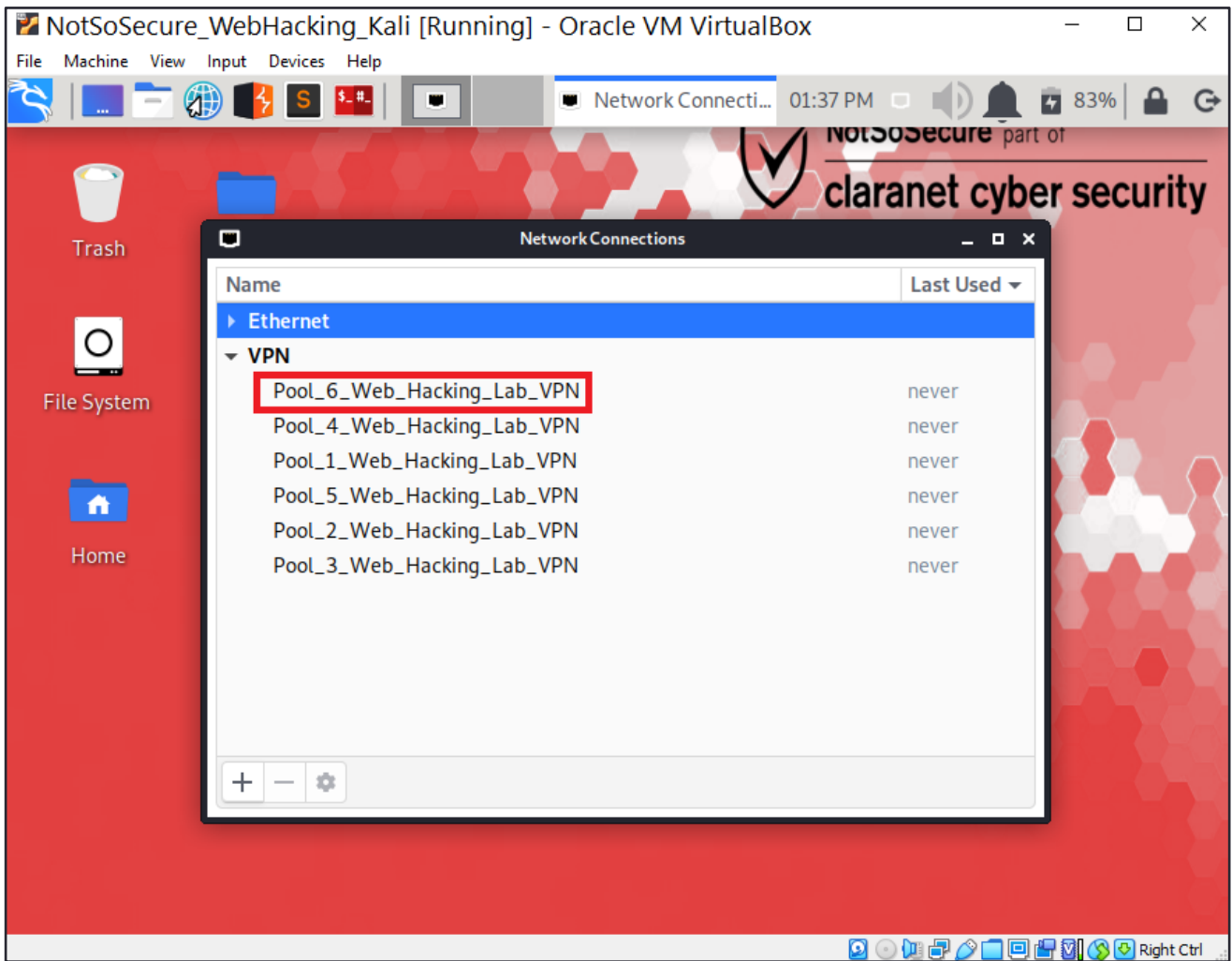
**Step 1:** Login using the following credentials. Click on the Network Connection icon at top right corner and select 'Configure VPN' under the 'VPN Connection' menu.

- **Username:** root
- **Password:** toor

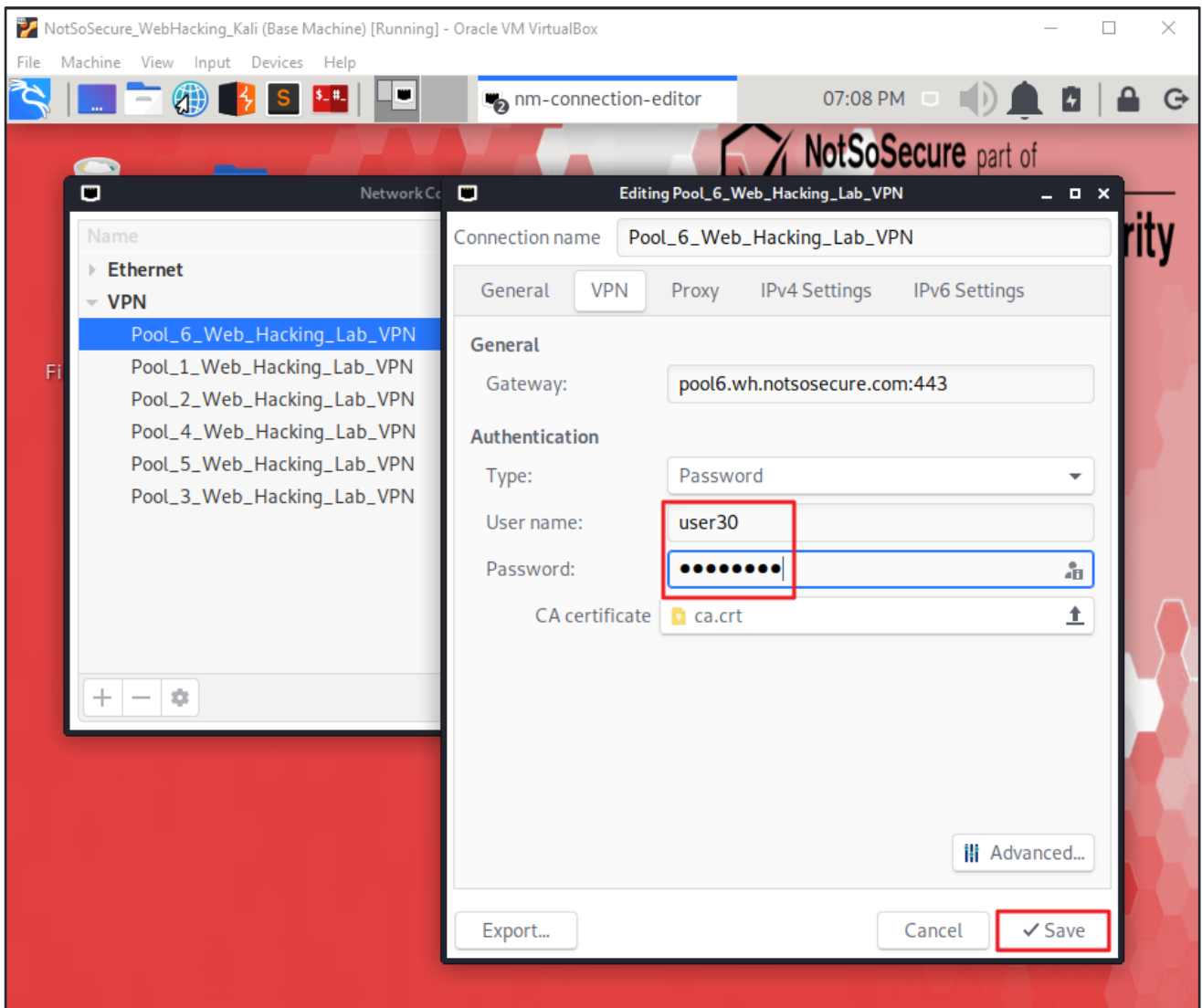




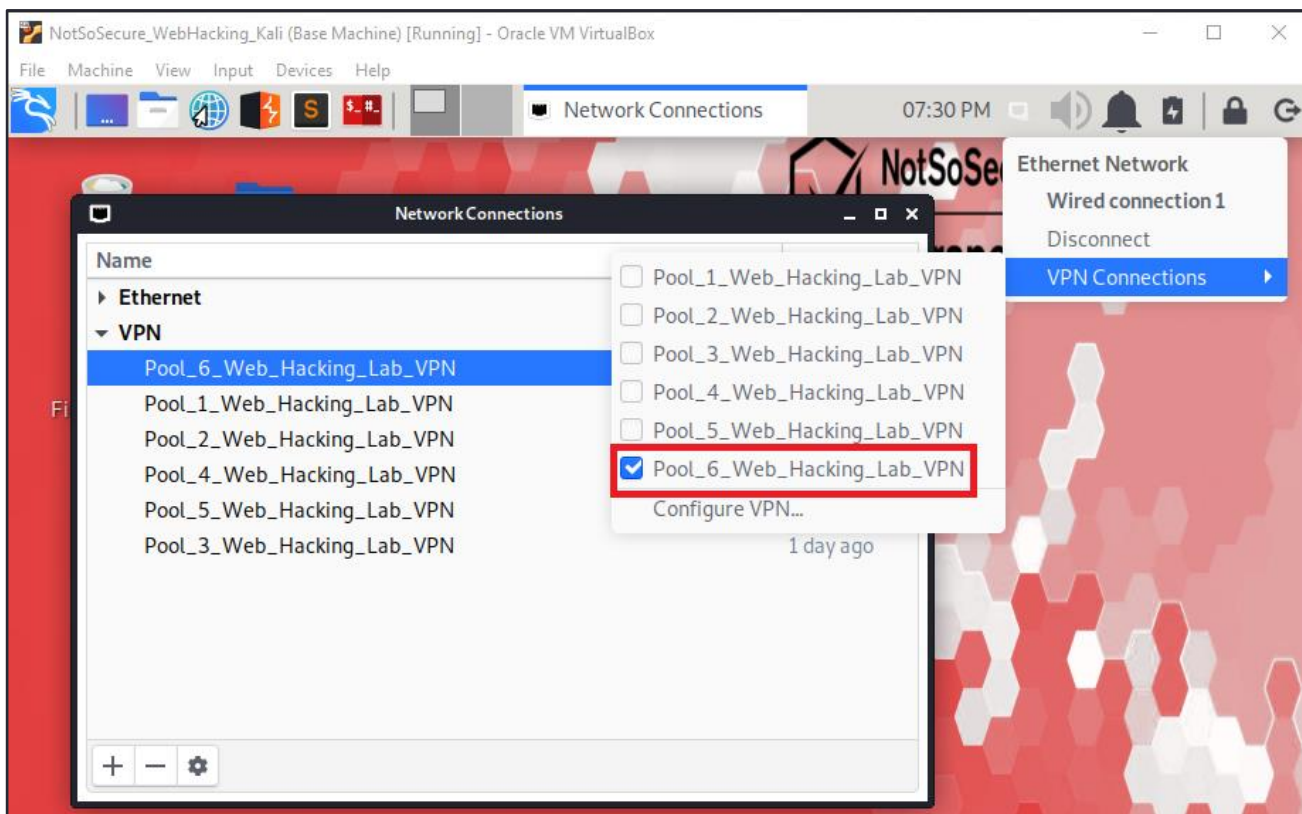
**Step 2:** Select the Pool mentioned in the student handout.



**Step 3:** Save the VPN username and password mentioned in the student handout.



**Step 4:** Again, click on the Network Connection icon at top right corner and select your Pool.



**Step 5:** Once connected to the VPN, an IP 192.168.4.X will be allocated to the machine, as shown below.

```
(root@kali)-[~]
└─# 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 08:00:27:80:13:f4 brd ff:ff:ff:ff:ff:ff
   inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85679sec preferred_lft 85679sec
   inet6 fe80::2e92:9646:d0d2:daf7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tap0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
   link/ether 5e:1a:ac:87:1e:b7 brd ff:ff:ff:ff:ff:ff
   inet 192.168.4.85/24 scope global tap0
       valid_lft forever preferred_lft forever
   inet6 fe80::5c1a:acff:fe87:1eb7/64 scope link
       valid_lft forever preferred_lft forever
```