

BHASIA Offensive OSINT

VM and VPN Instruction Sheet

How to Import the Virtual Machine Appliance

1. INSERT THE USB DRIVE.

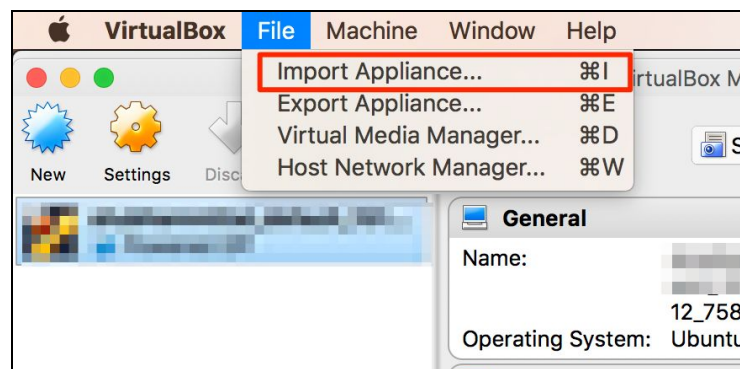
- A. Please make sure that USB is detected.
- B. Navigate to 'Appliance' folder in the USB Drive.
- C. Copy the BHAsia.OVA file to your Machine.

2. INSTALL VIRTUALBOX

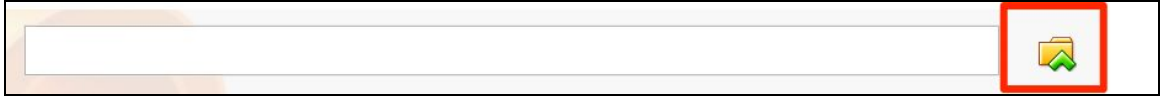
- A. Navigate to 'VirtualBox Installers' folder in the USB Drive.
- B. Depending on your platform, pick the VirtualBox installer.
 - i. Mac
 - ii. Windows
 - iii. Linux
- C. If VirtualBox is already installed in your machine, please make sure that you are using the latest version.
- D. If the installation process requires a restart, please restart your machine.

3. IMPORT THE OVA FILE

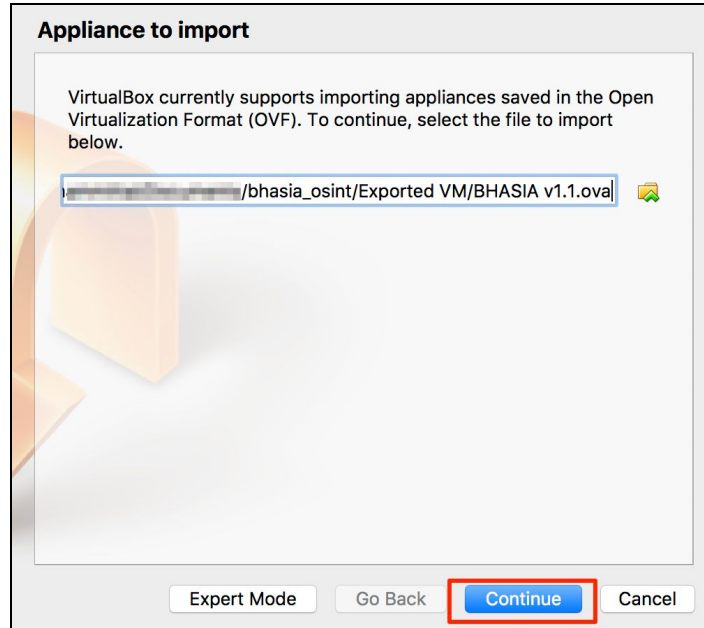
- A. Open VirtualBox.
- B. Go to 'File' in Menu bar and click on 'Import Appliance'.**



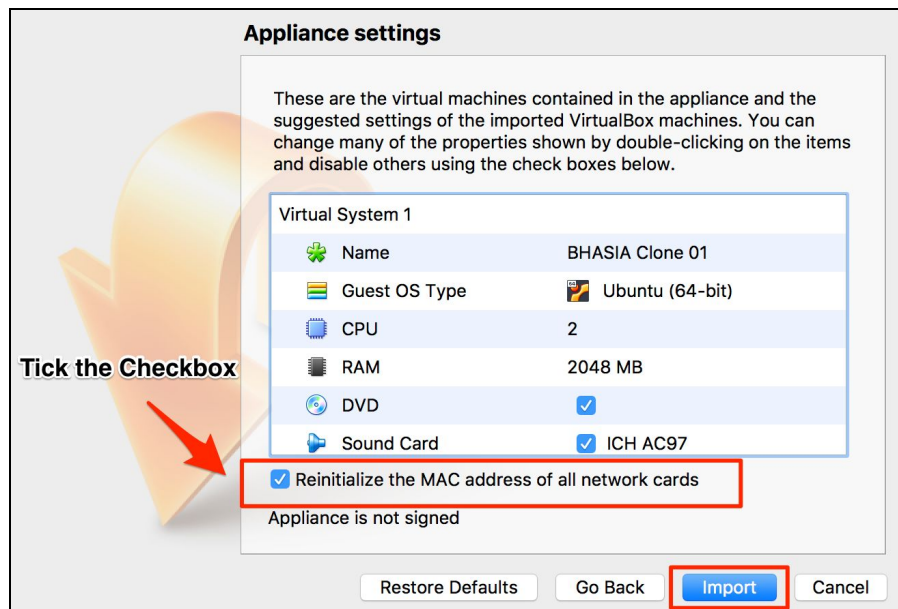
- C. Click on the Browse button, navigate to the path where you have copied the OVA File and click on **'Open'**.



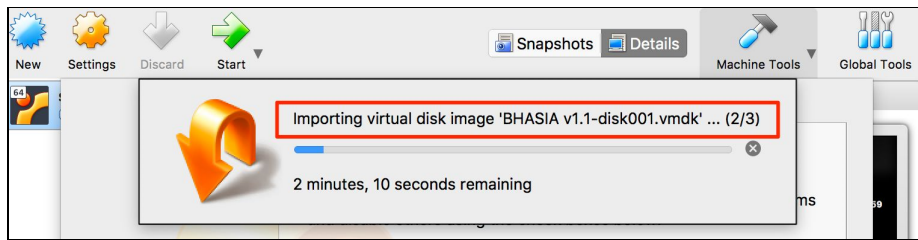
- D. Click on **'Continue'** (Do not go to Expert mode).



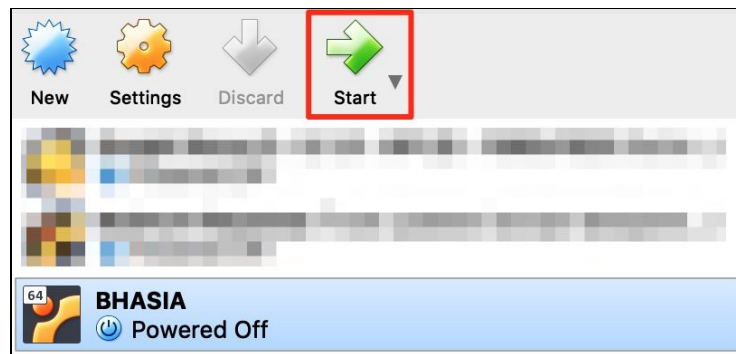
- E. Click on **'Reinitialize the MAC address of all network cards'** and then click on **'Import'**.



F. The Import process will start. Please wait.



G. Once the Import is done, VirtualBox will show the new VM. Select the VM and click on '**Start**' button in the panel.

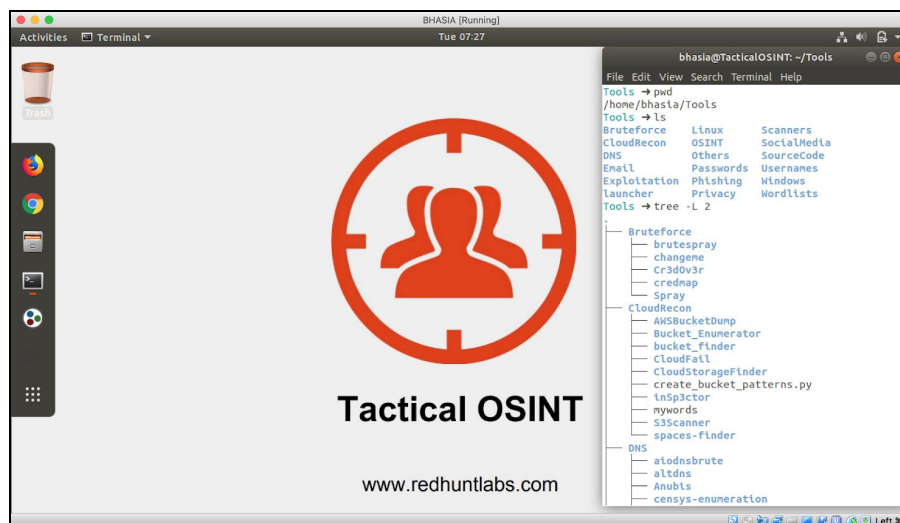


H. Username / Password the VM

Username: **bhasia**

Password: **bhasia**

I. Your VM is up and running.



Note: It is suggested to change the password after login, using the command 'passwd'.

How to Connect to the VPN

1. GO TO THE VPN FOLDER.

- A. Login into the VM and go to the folder /home/bhasia/VPN using the following command:

```
cd ~/VPN
```

```
bhasia@TacticalOSINT: ~/VPN
File Edit View Search Terminal Help
~ → pwd
/home/bhasia
~ → cd ~/VPN
VPN → ls
BHASIA_LAB_user10_LabVPNBHASIA.ovpn  BHASIA_LAB_user23_LabVPNBHASIA.ovpn  BHASIA_LAB_user35_LabVPNBHASIA.ovpn
BHASIA_LAB_user11_LabVPNBHASIA.ovpn  BHASIA_LAB_user24_LabVPNBHASIA.ovpn  BHASIA_LAB_user36_LabVPNBHASIA.ovpn
BHASIA_LAB_user12_LabVPNBHASIA.ovpn  BHASIA_LAB_user25_LabVPNBHASIA.ovpn  BHASIA_LAB_user37_LabVPNBHASIA.ovpn
BHASIA_LAB_user13_LabVPNBHASIA.ovpn  BHASIA_LAB_user26_LabVPNBHASIA.ovpn  BHASIA_LAB_user38_LabVPNBHASIA.ovpn
BHASIA_LAB_user14_LabVPNBHASIA.ovpn  BHASIA_LAB_user27_LabVPNBHASIA.ovpn  BHASIA_LAB_user39_LabVPNBHASIA.ovpn
BHASIA_LAB_user15_LabVPNBHASIA.ovpn  BHASIA_LAB_user28_LabVPNBHASIA.ovpn  BHASIA_LAB_user3_LabVPNBHASIA.ovpn
BHASIA_LAB_user16_LabVPNBHASIA.ovpn  BHASIA_LAB_user29_LabVPNBHASIA.ovpn  BHASIA_LAB_user40_LabVPNBHASIA.ovpn
BHASIA_LAB_user17_LabVPNBHASIA.ovpn  BHASIA_LAB_user2_LabVPNBHASIA.ovpn    BHASIA_LAB_user4_LabVPNBHASIA.ovpn
BHASIA_LAB_user18_LabVPNBHASIA.ovpn  BHASIA_LAB_user30_LabVPNBHASIA.ovpn  BHASIA_LAB_user5_LabVPNBHASIA.ovpn
BHASIA_LAB_user19_LabVPNBHASIA.ovpn  BHASIA_LAB_user31_LabVPNBHASIA.ovpn  BHASIA_LAB_user6_LabVPNBHASIA.ovpn
BHASIA_LAB_user1_LabVPNBHASIA.ovpn    BHASIA_LAB_user32_LabVPNBHASIA.ovpn  BHASIA_LAB_user7_LabVPNBHASIA.ovpn
BHASIA_LAB_user20_LabVPNBHASIA.ovpn  BHASIA_LAB_user33_LabVPNBHASIA.ovpn  BHASIA_LAB_user8_LabVPNBHASIA.ovpn
BHASIA_LAB_user21_LabVPNBHASIA.ovpn  BHASIA_LAB_user34_LabVPNBHASIA.ovpn  BHASIA_LAB_user9_LabVPNBHASIA.ovpn
```

- B. Connect to the VPN using the following command:

```
sudo openvpn BHASIA_LAB_userX_LabVPNBHASIA.ovpn
```

Note: **X** is your user id mentioned in the **handout**.

- C. Enter Your Username and Password mentioned in the **handout**:

```
VPN → sudo openvpn BHASIA_LAB_user16_LabVPNBHASIA.ovpn
Tue Mar 19 07:42:35 2019 DEPRECATED OPTION: --max-routes option ignored.The number of routes is unlimited as of OpenVPN 2.4. This option will
l be removed in a future version, please remove it from your configuration.
Tue Mar 19 07:42:35 2019 OpenVPN 2.4.4 x86_64-unknown-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [MH/PKTINFO] [AEAD] built on Mar  8 2018
Tue Mar 19 07:42:35 2019 library versions: OpenSSL 1.0.2n 7 Dec 2017, LZO 2.08
Enter Auth Username:user16
Enter Auth Password:
Tue Mar 19 07:42:40 2019 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Tue Mar 19 07:42:40 2019 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Tue Mar 19 07:42:40 2019 TCP/UDP: Preserving recently used remote address: [AF_INET]3.8.45.135:18265
Tue Mar 19 07:42:40 2019 UDP link local: (not bound)
Tue Mar 19 07:42:40 2019 UDP link remote: [AF_INET]3.8.45.135:18265
Tue Mar 19 07:42:40 2019 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Tue Mar 19 07:42:40 2019 VERIFY OK: depth=1, O=5c6e9e9323a7dc0b0f24798a, CN=5c6e9e9323a7dc0b0f24798a
Tue Mar 19 07:42:40 2019 VERIFY KU OK
Tue Mar 19 07:42:40 2019 Validating certificate extended key usage
Tue Mar 19 07:42:40 2019 NOTE: --mute triggered...
Tue Mar 19 07:42:40 2019 4 variation(s) on previous 3 message(s) suppressed by --mute
Tue Mar 19 07:42:40 2019 [5c6e9e9323a7dc0b0f24798a] Peer Connection Initiated with [AF_INET]3.8.45.135:18265
Tue Mar 19 07:42:42 2019 Data Channel: using negotiated cipher 'AES-128-GCM'
Tue Mar 19 07:42:42 2019 Outgoing Data Channel: Cipher 'AES-128-GCM' initialized with 128 bit key
Tue Mar 19 07:42:42 2019 Incoming Data Channel: Cipher 'AES-128-GCM' initialized with 128 bit key
Tue Mar 19 07:42:42 2019 TUN/TAP device tun0 opened
Tue Mar 19 07:42:42 2019 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Tue Mar 19 07:42:42 2019 /sbin/ifconfig tun0 192.168.222.28 netmask 255.255.255.0 mtu 1500 broadcast 192.168.222.255
Tue Mar 19 07:42:42 2019 Initialization Sequence Completed
```

Note: Do not close this terminal during the class. Also, your password will not be displayed in the terminal.

D. Once connected you will be able to open the website <http://carbonconsole.com>:

