Advanced Web Hacking

OVA Import & VPN Setup Guide



Contents

OVA	Import	.2
	For VirtualBox on Mac	.2
	For VirtualBox on Windows	.5
	For VirtualBox on Linux	. 8
VPN	Setup1	11



OVA Import

For VirtualBox on Mac

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

🗯 VirtualBox	File	Machine	Window	Help	
	Im	oort Applian	ice	۳	alBox
IN Tools	Ex Ne	oort Applian w Cloud VM	ice I	ЖE	
	Vir	tual Media N	Manager	ЖD	Ex
	по	SUNELWOIK	weicome	το ν	rtua
			The left par	rt of ap	plicat

Step 2: Browse to the downloaded ova file 'NotSoSecure_Web_Hacking_Training_2020.ova' and click Continue.

ource to import appliance from. This can be a l cloud VM from. le System to import the virtual appliance from. VirtualBox t (OVF). To continue, select the file to import b	local file sy	ystem to import C	VF archive or o	ne of known cloud	I service
le System to import the virtual appliance from. VirtualBox t (OVF). To continue, select the file to import b	x currently	v supports importi	ng appliances s	saved in the Open	\$
to import the virtual appliance from. VirtualBox t (OVF). To continue, select the file to import b	x currently	v supports importi	ng appliances s	aved in the Open	
	pelow.		0 11		
/Downloads/NotSoSecure_WebHacking_K	Kali.ova				
		Expert Mode	Go Bac	Continue	Canc
	/Downloads/NotSoSecure_WebHacking_	/Downloads/NotSoSecure_WebHacking_Kali.ova	/Downloads/NotSoSecure_WebHacking_Kali.ova	/Downloads/NotSoSecure_WebHacking_Kali.ova Expert Mode Go Bac	/Downloads/NotSoSecure_WebHacking_Kali.ova Expert Mode Go Back 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.

App	oliano	ce settings		
T c	hese hange	are the virtual machines cont e many of the properties show	ained in the appliance and the suggested settings of the imported VirtualBox machines. You can wn by double-clicking on the items and disable others using the check boxes below.	
١	/irtual	System 1		
	😽	Name	NotSoSecure_WebHacking_Kali	
	F	Product	NotSoSecure Web Hacking Custom Kali	
	F	Product-URL	https://notsosecure.com/hacking-training/advanced-web-hacking/	
	F	Vendor	NotSoSecure Global Services, A Claranet Group Company	
	F	Vendor-URL	https://notsosecure.com/	
	F	Version	2021v1	
	F	Description	Welcome to Advanced Web Hacking/ Web Hacking Black Belt Edition Training	
		Guest OS Type	💕 Ubuntu (64-bit)	
		CPU	3	
		RAM	4096 MB	
	$\overline{\mathbf{o}}$	DVD		
	Ø	USB Controller		
	Þ	Sound Card	✓ ICH AC97	
	-	Network Adapter	✓ Intel PRO/1000 MT Desktop (82540EM)	
	\diamond	Storage Controller (IDE)	PIIX4	
	\diamond	Storage Controller (IDE)	PIIX4	
	~ 🤌	Storage Controller (SATA)	AHCI	
		Virtual Disk Image	NotSoSecure_WebHacking_Kali-disk001.vmdk	
		Base Folder	/Users/WirtualBox VMs	
	a	Primary Group	1	
м	lachin	e Base Folder: 📄 /Users/	VirtualBox VMs	
N	AC A Addit	ddress Policy: Generate ne ional Options: 🗹 Import har	w MAC addresses for all network adapters d drives as VDI	\bigcirc
A	pplian	ce is not signed		
			Restore Defaults Go Back Import	Cancel

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

•••	Oracle VM VirtualBox Manager
Tools	New Settings Discard Start
VotSoSecure_WebHacking_Kali	General Preview Name: NotSoSecure_WebHacking_Kali Operating System: Ubuntu (64-bit)
	System Base Memory: 4096 MB Processors: 3 Boot Order: Optical, Hard Disk Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
	Display Video Memory: 16 MB Graphics Controller: VMSVGA Remote Desktop Server: Disabled Recording: Disabled
	Storage Controller: IDE IDE Secondary Device 0: [Optical Drive] Empty Controller: SATA SATA Port 0: NotSoSecure_WebHacking_Kali-disk001.vdi (Normal, 40.00 GB)
	Audio Host Driver: CoreAudio Controller: ICH AC97
	Network Adapter 1: Intel PRO/1000 MT Desktop (NAT)
	✓ USB
	USB Controller: OHCl Device Filters: 0 (0 active)
	Shared folders
	None
	Description
	Welcome to Advanced Web Hacking/ Web Hacking Black Belt Edition Training. The credentials for this machine is root:toor



For VirtualBox on Windows

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



Step 2: Browse to the downloaded ova file '**NotSoSecure_Web_Hacking_Training_2020.ova'** and click Continue.

~	Import Virtual Appliance
	Appliance to import
	Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.
	Source: Local File System
	Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.
	Eile: C:\Users Downloads\NotSoSecure_WebHacking_Kali.ova
	Expert Mode Next Cancel



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 contair properties shown by double-clicking or	ned in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of th n the items and disable others using the check boxes below.	ne
	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		
	🤌 USB Controller		
	🕪 Sound Card	ICH AC97	
	Network Adapter	Intel PRO/1000 MT Desktop (82540EM)	
	🔷 Storage Controller (IDE)	PIIX4	
	🔷 Storage Controller (IDE)	PIIX4	
	Y 🔶 Storage Controller (SATA)	AHCI	
	Virtual Disk Image	NotSoSecure_WebHacking_Kali-disk001.vmdk	
	📙 Base Folder	C:\Users\\VirtualBox VMs	
	🔞 Primary Group	1	
	Machine Base Folder: C:\Users	(VirtualBox VMs	~
	MAC Address Policy: Generate new M	MAC addresses for all network adapters	-
	Additional Options: 🗹 Import hard	drives as VDI	
	Appliance is not signed		
		Restore Defaults Import	Cancel

Step 4: Installation of the VM progresses.

Importing Appliance: Importing app	liance 'C:\Users $ imes$
Importing virtual disk image 'NotSoSecure_WebHa	acking_Kali-disk001.vmdk' (2/3) 7% 🗶
NotSoSecure part of claranet cyber security	[©] Claranet Cyber Sec

 $^{\odot}$ Claranet Cyber Security 2021. All rights reserved

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

🖸 Oracle VM VirtualBox Manager — 🗆 🗙					
<u>F</u> ile <u>M</u> achine <u>H</u> elp					
Tools	New Settings Discard Start				
64 NotSoSecure WebHacking Kali	📃 General 📃 Preview				
Powered Off	I System				
	Base Memory: 4096 MB Processors: 3 Boot Order: Optical, Hard Disk Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization				
	📃 Display				
	Video Memory: 16 MB Graphics Controller: VMSVGA Remote Desktop Server: Disabled Recording: Disabled				
	Storage				
	Controller: IDE IDE Secondary Master: [Optical Drive] Empty Controller: SATA SATA Port 0: NotSoSecure_WebHacking_Kali-disk001.vdi (Normal, 4	Ю.00 GB)			
	🕪 Audio				
	Host Driver: Windows DirectSound Controller: ICH AC97				
	Network				
	Adapter 1: Intel PRO/1000 MT Desktop (NAT)				
	🖉 USB				
	USB Controller: OHCI Device Filters: 0 (0 active)				
	Shared folders				
	None				
	Description				
	Welcome to Advanced Web Hacking/Web Hacking Black Belt Edition Training. The credentials for this machine is root:toor				
		•			



For VirtualBox on Linux

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

) [*]	Oracle VM Virt	ualBox Manager – 🗆 😣
<u>File M</u> achine <u>H</u> elp		_
Preferences	Ctrl+G	A R 🛱 🕂
💫 Import Appliance	Ctrl+I	nport Export New Add
🚯 Export Appliance	Ctrl+E	(internal Devid
🛛 🕝 <u>N</u> ew Cloud VM		
🔄 🗹 irtual Media Manager	Ctrl+D	application window
🔄 <u>H</u> ost Network Manager	Ctrl+H	and virtual machine
🖄 🖄 Network Operations Manager		computer. You can
▲ <u>R</u> eset All Warnings		ding toolbar buttons.
🕲 E <u>x</u> it	Ctrl+Q	tools of currently
	corresponding	element button.
	You can press t instant help, or <u>www.virtualbox</u> information and	he F1 key to get visit <mark>c.org</mark> for more d latest news.

Step 2: Browse to the downloaded ova file 'NotSoSecure_Web_Hacking_Training_2020.ova' and click Continue.

Import Virtual Appliance (×
Appliance to import	
Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.	J
Source: Local File System	•
Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.	I
File /home, // Downloads/NotSoSecure_WebHacking_Kali.ova	2
Expert Mode < Back Next > Cancel	



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 co can change many of the properti	ontained in the appliance and the suggested settings of the imported VirtualBox machines. You es 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)
СРИ	3
RAM	4096 MB
	✓
🤌 USB Controller	✓
🕩 Sound Card	✓ ICH AC97
Network Adapter	✓ 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: Ceperate	new MAC addresses for all network adapters
MAC Address Policy. denerate	
Additional Options: V Import f	hard drives as VDI
Appliance is not signed	
	Restore Defaults < Back

Step 4: Installation of the VM progresses.





Page | 9

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

	Oracle VM VirtualBox Manager	8
<u>F</u> ile <u>M</u> achine <u>H</u> elp		
Tools	Image: Weight of the sector	
	📃 General	Preview
Powered Off	Name: NotSoSecure_WebHacking_Kali Operating System: Ubuntu (64-bit)	
	System	
	Base Memory: 4096 MB Processors: 3 Boot Order: Optical, Hard Disk Acceleration: KVM Paravirtualization	NotSoSecure_WebHacking_Kali
	📃 Display	
	Video Memory: 16 MB Graphics Controller: VMSVGA Remote Desktop Server: Disabled Recording: Disabled	
	Storage	
	Controller: IDE IDE Secondary Master: [Optical Drive] Empty Controller: SATA SATA Port 0: NotSoSecure_WebHacking_Kali-dis	sk001.vdi (Normal, 40.00 GB)
	🕪 Audio	
	Host Driver: PulseAudio Controller: ICH AC97	
	Network	
	Adapter 1: Intel PRO/1000 MT Desktop (NAT)	
	🖉 USB	
	USB Controller: OHCI Device Filters: 0 (0 active)	
	Shared folders	
	None	
	Description	
	Welcome to Advanced Web Hacking/ Web Hacking Black Bel The credentials for this machine is root:toor	lt Edition Training.



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.





Page | 12
[©] Claranet Cyber Security 2021. All rights reserved

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

🏏 Not	SoSecure_WebHacking_Kali (Base Machine) [Running]	- Oracle VM VirtualBox				_		\times
	fachine View Input Devices Help	🍢 nm-connect	tion-editor	07:0	8 PM 🗆 🜓 🗴	0		G
				NotS	oSecure part o	f		
Fi	Name Ethernet VPN Pool_6_Web_Hacking_Lab_VPN Pool_1_Web_Hacking_Lab_VPN Dool_1_Web_Hacking_Lab_VPN	Connection name General VP General Gateway:	Pool_6_W N Proxy	eb_Hacking_Lab IPv4 Setting 5.wh.notsosecure	VPN s IPv6 Settings e.com:443	_ U	Î	ity
	Pool_2_Web_Hacking_Lab_VPN Pool_4_Web_Hacking_Lab_VPN Pool_5_Web_Hacking_Lab_VPN Pool_3_Web_Hacking_Lab_VPN	Authentication Type: Password User name: user30 Password: ••••••••			•			
	+ - \$	CA certifi	cate 🔽 ca.	crt		Ť	Ĵ	
		Export			Capcel	inced		
						Jave		



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

	Network Connections	07:30 PM	
Network Connec	tions	/ NotSoSe	Ethernet Network Wired connection 1 Disconnect
Ethernet VPN	Pool_1_Web_Hack Pool_2_Web_Hack Pool_2_Web_Ha	king_Lab_VPN king_Lab_VPN	VPN Connections
Pool_6_Web_Hacking_Lab_VPN Pool_1_Web_Hacking_Lab_VPN Pool_2_Web_Hacking_Lab_VPN Pool_4_Web_Hacking_Lab_VPN Pool_5_Web_Hacking_Lab_VPN	 Pool_3_Web_Hack Pool_4_Web_Hack Pool_5_Web_Hack Pool_6_Web_Hack Configure VPN_ 	king_Lab_VPN king_Lab_VPN king_Lab_VPN king_Lab_VPN	
Pool_3_Web_Hacking_Lab_VPN	1 da	yago	
+ - •			

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

(root kali)-[~]
L ip a
1: lo: <loopback,up,lower_up> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000</loopback,up,lower_up>
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</broadcast,multicast,up,lower_up>
link/ether 08:00:27:80:13:f4 brd 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</broadcast,multicast,up,lower_up>
link <u>/ether_5e:1a:ac:8</u> 7:1e:b7 brd 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



Page | 14

 $^{\odot}$ Claranet Cyber Security 2021. All rights reserved