

Ethical Hacking and Vulnerability Assessment

Roll No.: 18BCE152

Date: 28/07/2021

Practical 1

OBJECTIVE


- Study of Kali Linux and Lab setup.

INTRODUCTION

- **Kali Linux:** Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security. Kali Linux is mainly used for advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Many hackers use Kali Linux but it is not only OS used by Hackers. Security researcher and individual also can use for their purpose. Kali Linux is used by hackers because it is a free OS and has over 600 tools for penetration testing and security analytics.

- **Installation of kali Linux:**


For installation of kali go to the their official website <https://www.kali.org/get-kali/> Here you find various distribution of kali like ISO file, Mobile, Cloud, Live boot etc. Here I'm downloading kali for virtual machine.



Virtual Machines

- ✓ Snapshots functionary
- ✓ Isolated environment
- ✓ Customized Kali kernel
- ✗ Limited direct access to hardware
- ✗ Higher system requirements

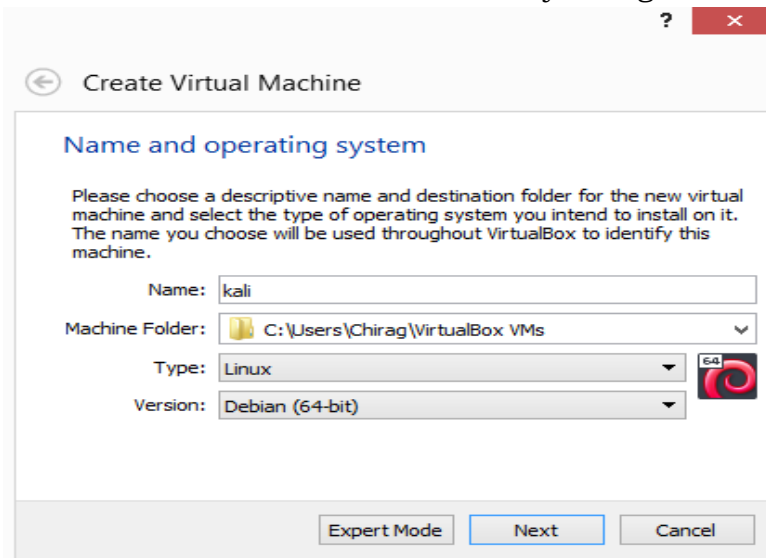
VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

 Recommended

Ethical Hacking and Vulnerability Assessment

Then install virtual box or VMware in your system. Go through below installation steps.

First Create new slot and do necessary configurations. Then install kali.





Create Virtual Machine

Name and operating system

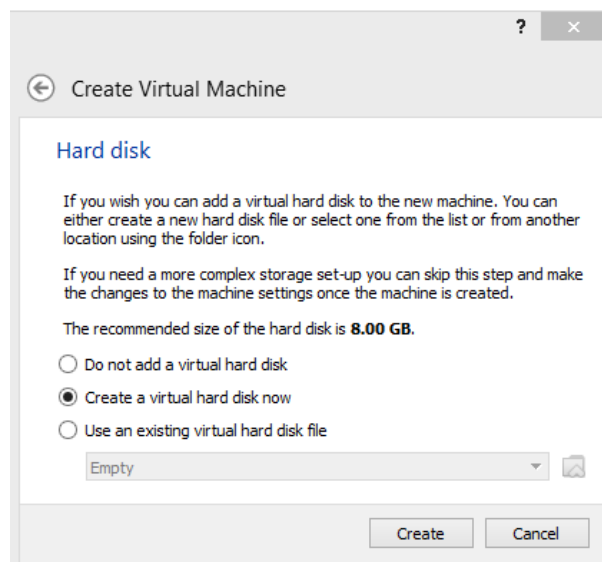
Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Machine Folder:  C:\Users\Chirag\VirtualBox VMs

Type: 

Version:



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

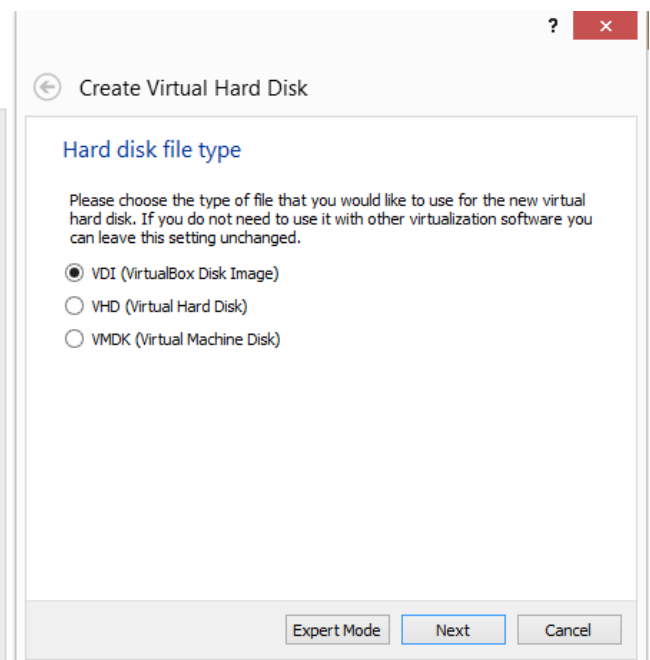
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

☐ Do not add a virtual hard disk

☒ Create a virtual hard disk now

☐ Use an existing virtual hard disk file



Create Virtual Hard Disk

Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

☒ VDI (VirtualBox Disk Image)

☐ VHD (Virtual Hard Disk)

☐ VMDK (Virtual Machine Disk)

Ethical Hacking and Vulnerability Assessment

- **Tools in kali:**

- 1. Information Gathering:**

- Nmap
- Zenmap
- Stealth scan

- 2. Vulnerability Analysis:**

- Bed
- Ohrwurm
- Powerfuzzer
- Sfuzz
- Siparmyknife

- 3. Web Application Analysis:**

- Burpsuite
- Httrack
- Sqlmap
- Vega
- Webscarab
- Wpscan

- 4. Database Assessment:**

- Bbqsl
- Jsql injection
- Oscanner
- Sqlmap
- Sqlninja
- Tmscmd10g

- 5. Password Attacks:**

- Crewl
- Crunch
- Hashcat
- John
- Johnny
- Medusa

- 6. Wireless Attacks:**

- Aircrack-ng
- Fern- wifi -cracker
- Kismet
- Ghost Phisher

- 7. Reverse Engineering:**

- Apktools
- Ollydbg
- Flasm

- 8. Exploitation Tools:**

- Armitage
- Metasploit
- Searchsploit
- Beef xss framework
- terminator

- 9. Sniffing and Spoffing:**

- Wireshark
- Bettercap
- Ettercap
- Hamster
- Driftnet

- 10. Post Exploitation:**

- MSF
- Veil -Pillage framework
- Powersploit

- 11. Forensics:**

- Autopsy
- Binwalk
- Galleta
- Hashdeep
- Volafax
- Volatility

- 12. Reporting Tools:**

- Dradis
- Faraday IDE
- Pipal
- Magictree

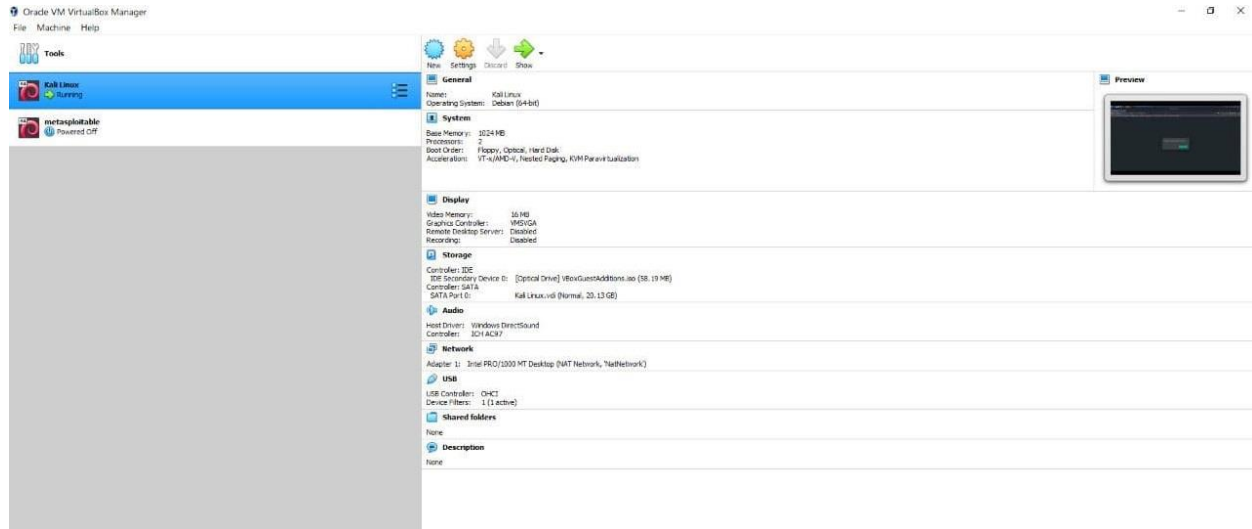
- 13. Social Engineering:**

- SET
- Backdoor-f
- U3-pwn
- Ghost Phisher

Ethical Hacking and Vulnerability Assessment

- **Metasploitable-Linux:**

Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques. The VM will run on any recent VMware products and other visualization technologies such as VirtualBox.



CONCLUSION

Kali Linux provide rich environment for ethical hacking and vulnerability assessment. It has wide variety of tools which make task easier. There is also metasploitable Linux environment which very good distribution for learning vulnerability assessment.