Ethical Hacking

Building Lab Lecture 2\_1 … 2\_

1. Install VirutalBox and It’s Extension pack, remove NetNetwork and add again
2. Download Extension 🡪 Open VirtualBox 🡪 Setting 🡪 Extension 🡪 Click add
3. Installing Kali Linux in VM 🡪 [www.offensive-security.com](http://www.offensive-security.com) 🡪 Download .ova file and

Click new appliance in VB 🡪 click import 🡪 I have add to [Rizwanwakil2017@gmail.com](mailto:Rizwanwakil2017@gmail.com) google drive.

1. Setup some properties of VM 🡪 give 2GB RAM to Kali VM
2. Make sure network is set to Network and enable promiscuous mode
3. Enter username (kali) with password (kali) and login

Download windows 10 ova file from Microsoft.com and make VM in VirtualBox or you can download from I have add to [Rizwanwakil2017@gmail.com](mailto:Rizwanwakil2017@gmail.com) google drive.

1. Make some properties adjustment and run the VM and give 2GB RAM to Win 10 VM
2. Make sure network is set to Network and enable promiscuous mode
3. Turn off firewall in windows and virus and threat protection

CREATING SNAPSHOT IN VIRTUALBOX

1. Shutdown the system and click on take snapshot
2. Create snapshot of both Kali & Win VM to restore in case something go wrong

BASIC KALI LINUX COMMAND

1. In GitHub of [Rizwan.wakil2020@gmail.com](mailto:Rizwan.wakil2020@gmail.com) have complete Linux tutorial document

HOW TO BE ANONYMOUS ONLINE

1. How network work, all device connected to router 🡪 router give ip to devices 🡪

Then router is connected to local ISP 🡪 ISP is connected to internet

1. When can check our public IP by check on google what is my public IP
2. How to change DNS servers in Kali

Open terminal 🡪 cat /etc/resolv.conf

Now open vi /etc/dhcp/dhcpclient.conf

Uncomment the line prepend domain-name and enter

Three DNS IP separated by comma with space

209.244.0.3, 64.6.64.6, 8.8.8.8;

4. restart the network services using command

Service network-manager restart

1. Now check again the vim /etc/resolv.conf

HOW TO USE VPN IN KALI LINUX

1. First we need to disable web rtc 🡪 open firebox 🡪 type about:config in address bar

Then search for media.peerconnection.enable 🡪 make value to false

1. In googel search for free VPN book 🡪 open [www.vpnbook.com](http://www.vpnbook.com) 🡪 click on openvpn

Download any server 🡪 extract the file 🡪 using terminal

1. After extracting 🡪 type openvpn file\_name
2. Enter the username and password provided by vpnbook.com website
3. Make sure by check the public ip address
4. Check by dns leakage test [www.dnsleaktest.com](http://www.dnsleaktest.com) will show location and IP

HOW TO BROWSE DARKWEB

1. There are three level of website
   1. Visible Web which we are accessing for normal public
   2. Deep Web to access deep web we need special tools and accessible to government website
   3. Dark Web here are dirty website are there. We need some special tool to access dark website
2. Download TOR on Kali and Install on it

Make sure VPN is connected

apt-get install tor -y

run above command to install TOR

now open google and search tor browser download

download and install on system

[www.torproject.org](http://www.torproject.org) and download it

open folder and edit the start-desktop file and comment the root user condition

now run the tor browser and it will work this time

1. Configure tor browser and choose safest option
2. Open DuckDuckgo.com and search for hidden wiki

PENTRATION TESTING IN KALI LINUX

1. We need kali Linux compatible USB Wireless adaptor

HOW TO CHANGE MAC ADDRESS

1. We are using mac changer to change mac address
2. First down the connection then run the macchanger command
3. Run the command macchanger –help
4. macchanger –random device

MONITOR MODE VS MANAGED MODE

1. by default system is in managed mode
2. to change from managed mode to monitor mode, run the below command

airmon-ng start wlan0mon. or iwconfig wlan0 mode monitor

1. if the interface is in monitor mode, it can not connect to network, but can analysis the traffic.
2. Ifconfig and iwconfig command is used to determine the interface mode
3. to change from monitor mode to managed mode, run the below command

airmon-ng stop wlan0mon or iwconfig wlan0 mode managed

GATHERING INFORMATION FROM NETWORK WITHOUT CONNECTION TO NETWORK

1. Connect to Kali Linux and check the wireless adaptor status
2. By running command iwconfig wlan0
3. Change to mode to monitor mode by running below command
4. airmon-ng start wlan0mon or iwconfig wlan0 mode monitor
5. run below command to get information

airodump-ng wlan0mon

1. after some time 30 sec press CTRL+C and analysis the information
2. PWR stand for Power , represent the signal status
3. To get more information information about route issue below command

Airodump-ng –channel 9 –bssid mac\_addr\_of\_router –write test1 wlan0mon

Above command will give more information and show all connected devices as well

1. Open test1 file using wireshark for more analysis

HOW TO DISCONNECT A DEVICE FORM ROUTER

1. Login to kali and run below command
2. airodump-ng –channel 9 –bsid mac\_address wlan0mon
3. this will give mac address to target device
4. open another terminal window
5. issue below command to disconnect device

aireplay-ng –deauth 10000 -a router\_mac\_addr -c client\_mac\_addr wlan0

CRACKING NETWORK PASSWORD

Encryption models

There are two encryption protocol used in routers

WEP (Wire equivalent privacy ) this is old way and not safe

WPA / WPA2 (wi-fi protection access) this is latest protocol

Cracking WEP

Fake authentication

Packet Injection

How WPA works?

Capturing Handshakes

Creating WordLists

WPA Live Cracking

Safe Routers