

NAME: KARABO JOSEPH

ID: UM84565SEN93784

COURSE:

ETHICAL HACKING TECHNIQUES AND TOOLS PART 1

Table of Contents

1	INTRODUCTION .....	3
2	OBJECTIVES .....	4
3	THEORY .....	4
3.1	MEANING OF KALI LINUX .....	4
3.2	INSTALLATION OF KALI LINUX .....	6
3.3	THE BASIC COMMAND IN LINUX .....	8
3.4	NAVIGATING THE FILES .....	10
3.5	UPDATING KALI LINUX .....	12
3.6	KALI LINUX TOOLS .....	14
3.7	INFORMATION GATHERING AND RECONNAISSANCE .....	14
3.7.1	Open source intelligence .....	15
3.7.2	Maltego .....	15
3.7.3	Nmap and ZenMap .....	17
3.8	PENETRATION .....	17
3.8.1	Hydra .....	18
3.8.2	John the Ripper .....	20
4	CONCLUSION .....	22
5	Bibliography .....	24

## 1 INTRODUCTION

In modern day world we cannot do away with using computers to run successful business. Computer are used in business for internal and external communication using emails, video conferencing, word processing and many more, there are used as well as to store data, to research and make trademarks this are but a few uses of computers in business. For these to be possible or made easy computers need to be networked in order to facilitate an exchange of information internally and externally, meaning that isolated computers are not enough on their solitude to achieve much. When we connect them to a network we risk them to be exposed to the outside world and there can be hacked. Hacking essentially implies the use of computers to carry out malicious acts, for instance, stealing personal or corporate data, privacy invasion, fraud, and so on, cybercrimes are known to cost organizations all around the world millions of dollars each year (Fletcher, 2019, p. 10).

Hackers was a word used to describe individual's experts who had the skills and ability to change mainframe systems by re developing them therefore increasing their efficiency and allowing them to carryout multiple tasks. Now in modern times the term is used to describe an expert programmer who can gain an unauthorized access into computer networks by exploiting weakness in the system or network in order to gain by using mischief and malice. Hackers have the ability to crack passwords, to penetrate networks or even intercept or stop network services. The main reason for unethical hacking is to gain information or finances by stealing. Even though that is the case not all hacking is bad, ethical hacking is an authorized practice of detecting weakness in application and networks and potential data breaches. Ethical hacking aims at strengthening the network from point that unauthorized hackers can exploit. Basically the ethical hackers improves the ethical hackers improve the security of the systems to withstand attacks.

The practice of ethical hacking is called white hat hacking and in contrast to black hat hackers who are those who violate security by using illegal techniques to compromise the systems. The difference between the type of hacking the motive or the intent (Boteanu, 2011). White hat hackers hack to remedy the network from weakness so as to prevent black hat hackers from taking advantage. The black hat hacker is motivated by mischievous intent to gain profit or information and to harass. White hat hackers duplicate the techniques and tools followed by malicious hackers in order to find the systems vulnerabilities. There use tools to perform the tasks. Ethical hacking is tied to a certain operating system called kali Linux. It contains many tools within used for reverse engineering, for auditing and penetration test. This report focuses on the Linux architecture how is built, components that make Kali and what really kali Linux is. The paper focus on the function of the platform and the capabilities of the tools it contains. Lastly report focuses on the Kali linux platform is used, new features and the installation of kali Linux.

## 2 OBJECTIVES

To learn Linux architecture and ubiquity

To know what is kali Linux and why should it be used

To learn the new features

## 3 THEORY

### 3.1 MEANING OF KALI LINUX

Kali Linux is the most widely used and advanced penetration testing distribution system. It is an open source, Debian-based Linux system used for penetration testing, security

research, computer forensics and reverse engineering. Kali Linux has an information security organization behind it and it is called the offensive security. It develops, funds and maintain Kali Linux. Kali Linux boast of over 600 tools used for penetration testing (Fletcher, 2019).

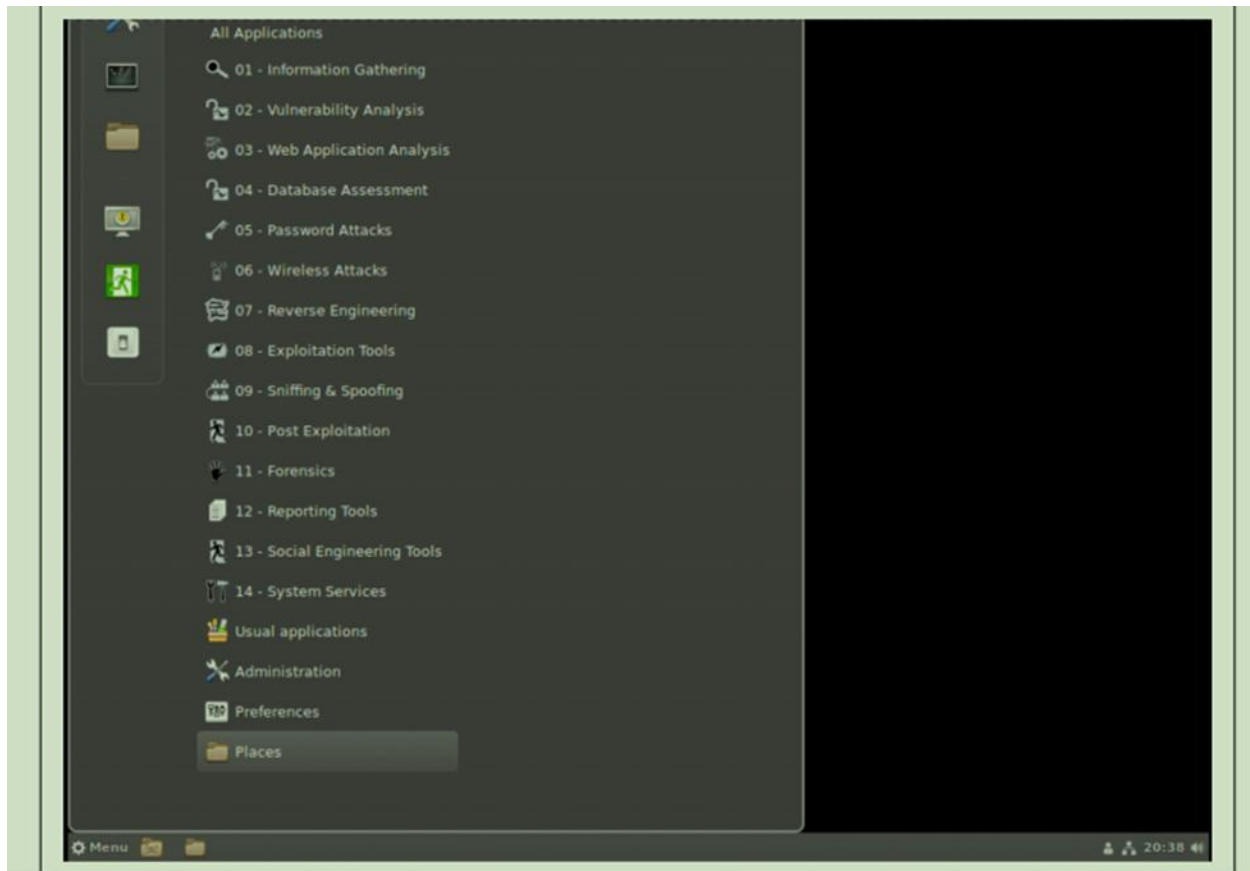


Figure 1: showing the function that can be done with kali Linux

Kali Linux is not mainly about the tools it has, nor the operating system but it's a platform and can be used by anyone. Kali Linux can easily be customized by anyone to meet their needs and preferences. The platform can run in wide range of devices or hardware. It support wireless interfaces because it has been engineered with many platforms to do so.

### 3.2 INSTALLATION OF KALI LINUX

Kali Linux is one of the best security platforms of an ethical penetration testing, containing a set of tools divided by the categories. It is an open debian source and its official webpage is <https://www.kali.org>. Kali Linux can be installed in any hardware and become the operating system. Installation of the platform is a practical option because it provide more option to combine tools (Tutorial point, 2018). Virtual Box a software that can be used to run Kali Linux it specializes in virtualizing various operating systems, it can be used or installed in Windows, any Linux as well. When the site is reached many platforms can be downloaded from there (hoffman, 2020) .

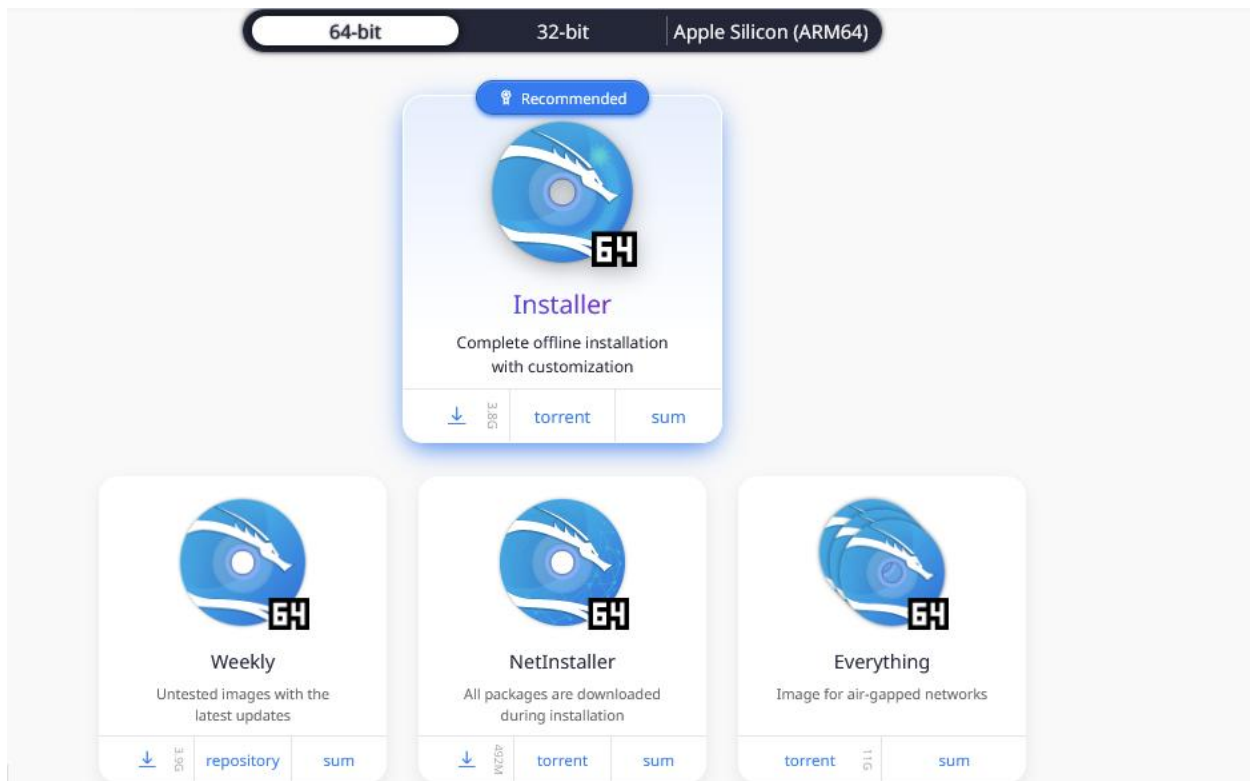


Figure 2: a picture showing the download package (kali Linux , n.d.)

The easiest way to install the platform is to visit the webpage and from there, their instruction on what package to choose based on preference and capabilities of your virtual machine. The Kali installation process is simple. The settings available to other

distributions are not available to you. Package categories won't be chosen by you. Kali installs a predetermined set of packages. You begin with a very complete range of tools for security testing or forensics, and you can add more or even remove some later. Configuring entails choosing a disk to install on and formatting and partitioning it. In addition, you must setup the network, including the host name and whether DHCP or a static address is being used. The programs will update and you will be prepared to boot into Linux after you have configured that, set your time zone, and made a few other basic setup adjustments. Once the virtual machine has been fully constructed, you must navigate to the settings and make sure that the Network settings are adjusted by selecting to bridge the virtual machine to your router. After completing the configuration, the image ought to boot up.

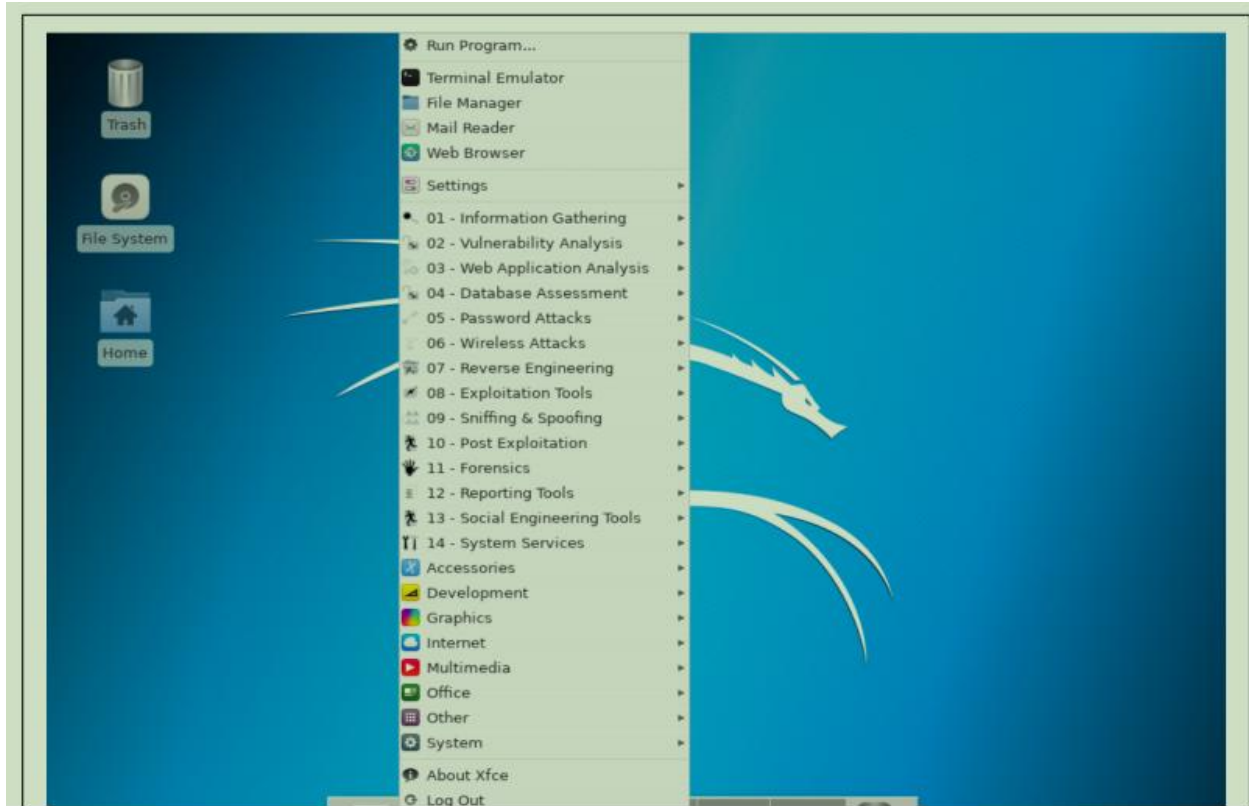


Figure 3: showing the application menu

### 3.3 THE BASIC COMMAND IN LINUX

Unlike Windows or mac OS, Linux's command line does not always indicate the directory you are currently in. Generally, you need to know where you are in order to browse to a new directory. The program `pwd`, which returns the current working directory, locates you within the directory structure.

The command you need to type is

“Startx”



Then press the Enter key. This will begin the process of installing the hard drive's GUI (Graphical User Interface), which is also advised. You have to answer a few questions about language, keyboard, location, and clock settings for the time zone until the GUI is installed. To get the image to boot from the hard drive after the installation is finished, you have to restart it. Following the reboot, Kali will prompt you to provide your CLI login credentials. For the username, type

“Root”

And see the password type

“toor”

And press the Enter key. Don't worry if you're new to the CLI and are unsure of which commands to type. You can always type the command to switch to the GUI.

“startx”

Press the Enter key. This will launch the intuitive graphical user interface (GUI) and provide you access to all of the Pen Test tools that we will cover in more detail later. IP addressing is one of the other fundamental settings you must make. By default, Kali Linux looks for your DHCP IP address. However, it's best to assign a static IP address so you always know which IP address belongs to which machine. You must use the following CLI command in Kali to assign an IP address:

“Ifconfig eth0 10.10.10.2/24 up”

The IP address of your router serves as the default gateway, which needs to be configured next. Enter the command

“Route add default gw 10.10.10.1”

To accomplish that. Once these configurations are finished, use the command

“Ping 10.10.10.1”

To check the IP address of your router. After you can reach your default gateway and use that router to access the internet, you should use the following command to check your internet connectivity:

“Ping [www.google.com](http://www.google.com) “

In the event that this is accomplished, your virtual Kali Linux installation is online. It is necessary for you to have internet access in order to upgrade Kali Linux. The first thing you should do is update Kali Linux. Updating your operating system should be your first step following a clean install. By exploring repositories and installing or updating packages along with all necessary dependencies, Advanced Packaging Tools, also known as APT, expands the functionality of Debian packages.

### 3.4 NAVIGATING THE FILES

Using the terminal to navigate the file system is a fundamental Linux ability. You must be able to navigate around to seek files, directories, and applications hidden in other directories if you are to accomplish anything. The directories are visible while using a GUI-based system, but when using the command-line interface, the structure is fully text-based, and accessing the file system requires executing certain commands.

Changing directory with cd

Use the change directory command (cd) to modify directories from the terminal. Here's an example of how to change to the configuration file storage directory, /etc.:

```
kali >cd /etc.
```

```
root@kali:/etc#
```

When we navigate to the /etc. directory, the prompt changes to root@kali:/etc. We can enter pwd to verify this.

```
root@kali:/etc# pwd /etc
```

We use `cd` followed by double dots (`..`) to advance one level up in the file structure (toward the file structure root, or `/`), as demonstrated here:

```
root@kali:/etc# cd ..
```

```
root@kali:/# pwd
```

```
/
```

```
root@kali:/#
```

From `/etc.` to the `/root` directory, this advances us one step; you can advance whatever number of levels as necessary. Simply apply the same number of double-dot pairings to the desired number of levels moved: To go up a level, you would utilize `..`. To go up two levels, you would utilize `...`. To advance three levels, you would require `....`. And so forth. For instance, to advance two levels, type `cd`, then two sets of double dots separated by a space, like this:

```
Kali >cd...
```

Alternatively, you can use the command `cd /`, which denotes the file system's root, to navigate to the root level of the file structure from any location.

### Listing the Contents of a Directory with `ls`

To see the contents of a directory (the files and subdirectories), we can use the `ls` (list) command. This is very similar to the `dir` command in Windows.

```
kali >ls
```

```
bin initrd.img media run var
```

```
boot initrd.img.old mnt sbin vmlinuz
```

dev lib opt srv vmlinuz.old

etc lib64 proc tmp

home lost+found root usr

```
kali >ls
bin  initrd.img  media  run  var
boot initrd.img.old  mnt    sbin  vmlinuz
dev  lib         opt    srv   vmlinuz.old
etc  lib64       proc   tmp
home lost+found  root   usr
```

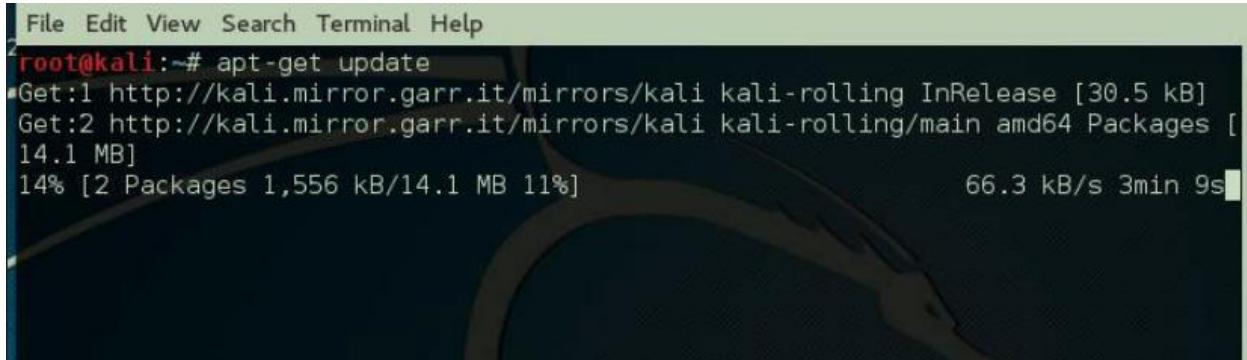
Figure 4: the output of the ls command

This command lists both the files and directories contained in the directory. You can also use this command on any particular directory, not just the one you are currently in, by listing the directory name after the command; for example, ls /etc. shows what's in the /etc. directory

### 3.5 UPDATING KALI LINUX

It very important to use a newer version so as not to miss out on the new features and tools that might prove worth of installing. Since technology changes on a day to day basis the newer version will have those features and tools that meet the relevant need at time to remain functional.

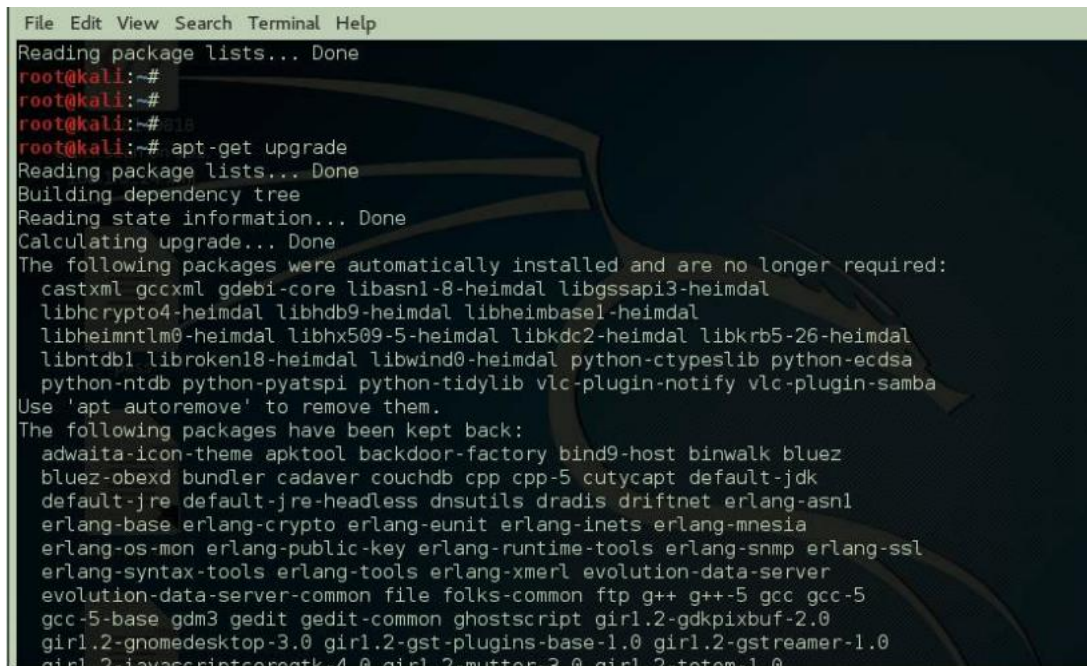
First, select Application -> Terminal. After that, type "apt-get update," and the update will happen as picture below indicates.



```
File Edit View Search Terminal Help
root@kali:~# apt-get update
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [
14.1 MB]
14% [2 Packages 1,556 kB/14.1 MB 11%] 66.3 kB/s 3min 9s
```

Figure 5: shows update in the command prompt

Secondly to upgrade the tools, you type “apt-get upgrade” then the new packages will be downloaded



```
File Edit View Search Terminal Help
Reading package lists... Done
root@kali:~#
root@kali:~#
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
castxml gccxml gdebi-core libasn1-8-heimdal libgssapi3-heimdal
libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal
libheimntlm0-heimdal libhx509-5-heimdal libkdc2-heimdal libkrb5-26-heimdal
libntdb1 libroken18-heimdal libwind0-heimdal python-ctypeslib python-ecdsa
python-ntdb python-pyatspi python-tidylib vlc-plugin-notify vlc-plugin-samba
Use 'apt autoremove' to remove them.
The following packages have been kept back:
adwaita-icon-theme apktool backdoor-factory bind9-host binwalk bluez
bluez-obexd bundler cadaver couchdb cpp cpp-5 cutycapt default-jdk
default-jre default-jre-headless dnsutils dradis driftnet erlang-asnl
erlang-base erlang-crypto erlang-eunit erlang-inets erlang-mnesia
erlang-os-mon erlang-public-key erlang-runtime-tools erlang-snmp erlang-ssl
erlang-syntax-tools erlang-tools erlang-xmerl evolution-data-server
evolution-data-server-common file folks-common ftp g++ g++-5 gcc gcc-5
gcc-5-base gdm3 gedit gedit-common ghostscript girl1.2-gdkpixbuf-2.0
girl1.2-gnomedesktop-3.0 girl1.2-gst-plugins-base-1.0 girl1.2-gstreamer-1.0
girl1.2-javascriptcoregtk-4.0 girl1.2-mutter-3.0 girl1.2-totem-1.0
```



Figure 6: showing the downloading packages

Thirdly, a question will pop up asking if you want to continue, to continue. Type “y” and “Enter”

Lastly, upgrading the new version of Operating System, type “apt-get dist-upgrade”.

```
root@kali:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
caribou-antler castxml creepy dff gccxml gdebi-core girl.2-clutter-gst-2.0 girl.2-evinced-3.0 girl.2-gkbd-3.0
girl.2-packagekit-glib-1.6 girl.2-xxl-1.0 gnome-icon-theme-symbolic gnome-packagekit gnome-packagekit-data
gtk2-engines guicharmap hwdetect libapache2-mod-php5 libasnl-8-heimdal libavcodec-ffmpeg56 libavdevice-ffmpeg54
libavfilter-ffmpeg5 libavformat-ffmpeg56 libavresample-ffmpeg2 libavutil-ffmpeg54 libbasicusageenvironment0
libbind9-98 libboost-filesystem1.58.0 libboost-python1.58.0 libboost-python1.61.6 libboost-system1.58.0
libboost-thread1.58.0 libcamel-1.2-54 libchromaprint0 libclutter-gst-2.0-0 libcrypto++9v5 libcurl-perl
libcurl3-gnutls libdata-wiretap-perl libdbd-oracle-thinclient-perl libdbd-sqlite-perl libdbi-perl libdict-1.0-9
libglew1.13 libgrilo-0.2-1 libgroupsock1 libgsasl3-heimdal libgtkglext1 libguicharmap-2-98-7
libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhunspell-1.3-8
libhx509-5-heimdal libical2 libilmbase6v5 libisc95 libisc98 libisc99 libjasper-perl libjpeg9
libkdc2-heimdal libkrb5-26-heimdal liblist-moreutils-perl liblivemedia23 libllvm3.7 liblouis9 liblwres98
libnm-glib-vpn1 libntdb1 libonig2 libopenexr6v5 libopenjpeg5 libpff1 libpnm-5.1-0 libphonon4 libpoppler57
libpostproc-ffmpeg53 libpth20 libqdbm14 libqmi-glib1 libquvi-scripts libquvi7 libradare2-0.9.9 libregfi0
libroken18-heimdal libsodium13 libswresample-ffmpeg1 libswscale-ffmpeg3 libtask-weaken-perl libtre5 libtrie0
libusageenvironment1 libvpx3 libwebp5 libwebpdemux1 libwebpmux1 libwebRTC-audio-processing-0 libwildmidi1
```

Figure 7: the update of packages has been done

### 3.6 KALI LINUX TOOLS

The kali Linux penetration testing platform contains a many set of tools. From information gathering, re-engineering, computer forensics, and to final reporting. The platform allows security experts and IT professionals to assess the security of their system through penetration testing.

### 3.7 INFORMATION GATHERING AND RECONNAISSANCE

Any task you do that involves penetration testing, ethical hacking, or security assessment usually requires guidelines. These might contain all of the targets, although they frequently don't. You must decide what your goals are, taking into account both system and human ambitions. You'll need to conduct what's known as reconnaissance in order to accomplish that. Attacks can target individuals in addition to systems and the programs that operate on them. Although it's not a guarantee, you might be requested to carry out social engineering attacks. Social engineering attacks are, after all, by far the most prevalent types of compromise and penetration that occur these days.

According to some estimates (Messier, 2018), such as those from Verizon and Fire Eye, social engineering is to blame for 80–90%, if not more, of the data breaches that occur in businesses today.

### 3.7.1 Open source intelligence

Open source intelligence: what is it? Everything you discover from a public source, be it official documents that could be deemed public (like real estate transactions) or information obtained from other public sources (like mailing list archives) that are regarded as open sources of data. Although software may come to mind when you hear the term "open source," other types of information can also benefit from it.

### 3.7.2 Maltego

I'm a command-line guy since my experience dates back a long way to a time before GUIs were invented. Yes, Kali comes with a plethora of command-line tools. However, some folks are just GUI types. Thus far, we have examined numerous programs that can extract large amounts of data from open sources. Easy insight into the relationships between the various bits of information is something that the tools we have utilized up to this point have not provided. Additionally, we are not given a quick and simple way to pivot a piece of data we already have in order to obtain more information.

It might be simpler to just choose a piece of data and then run that other module on it rather than taking the Harvester's output of our list of contacts and feeding it into yet another tool or module. This is the role of Maltego. A GUI-based application called Maltego performs some of the tasks we have previously completed. With Maltego, on the other hand, all of the relationships between the entities are displayed clearly because we can view it in a graph-based structure (Messier, 2018). After we have a

subset of the entities, we can obtain more information from those things. Subsequently, this may lead to other information, which may subsequently lead to even more information, and so on. Many additional transformations from various sources are included in the commercial edition. Nevertheless, we may still install a number of transforms using the community edition. Figure 5 displays the list of transform bundles.

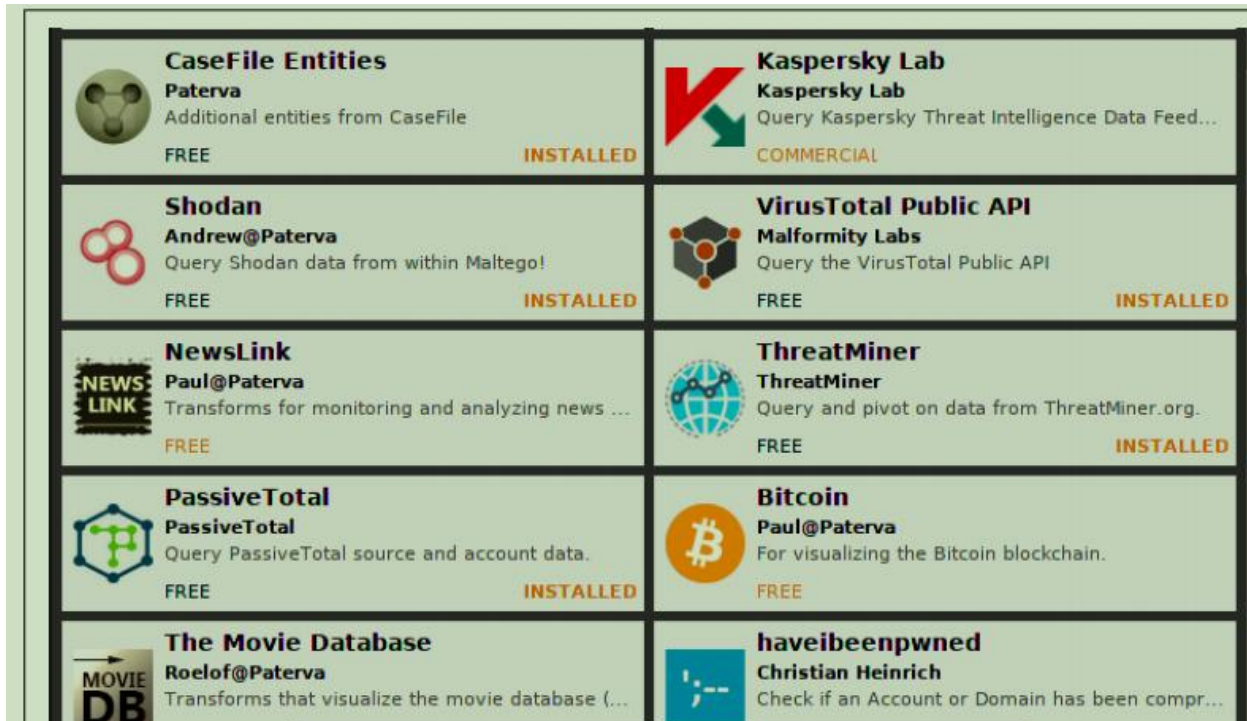


Figure 8: shows a list of packages in Maltego

Maltego does work with transforms. A transform is a segment of Maltego Scripting Language (MSL) code that creates one entity from another by utilizing a data source. For example, suppose you have a hostname entity. The installed transformations serve as Maltego's engine. Nevertheless, you don't have to apply each change one after the other to do the job yourself. A device known as a machine is used to accomplish this. It is possible to build a machine that applies transforms from an initial state. We can obtain a company's footprint, for instance. The device that will handle the task for us consists of transforms that can locate connections between systems and perform DNS



lookups. Based on a given domain, the Footprint L3 machine executes transforms to obtain the mail exchanger and name server records (Messier, 2018). It then extracts IP addresses from hostnames and performs further branching out, searching for more similar and related IP addresses and hostnames.

### 3.7.3 Nmap and ZenMap

NMAP and ZenMAP are helpful programs for Kali Linux ethical hacking scanning. Though ZenMAP includes a graphical user interface (GUI), NMAP is essentially the same program as ZenMAP. NMAP is a free utility program for security audits and network discovery. It is also helpful for many systems and network managers for activities like scheduling service upgrades, keeping track of host or service uptime, and inventorying the network. NMAP makes use of raw IP packets in new ways to find hosts on the network, the services (name and version of the application) those hosts are providing, the operating systems (and versions) those hosts are running, the kinds of firewalls and packet filters that are in place, etc.

## 3.8 PENETRATION

Many people may associate security testing with penetration testing, in which the objective is to gain access to systems and elevate one's privileges. When experts discuss security, and certifying bodies especially do so, they always bring up the so-called trio. The three pillars of information security—confidentiality, integrity, and availability—are what set it apart from others. The security of any software or system is affected by anything that could affect any one of these features. Security testing will or should include all of those factors, rather than just the narrow perspective that a penetration test might reveal.

The triad is commonly depicted as an equilateral triangle, as you may be aware. Since the three elements are deemed to have equal weight, the triangle is equilateral. Furthermore, you are left without a triangle if any of the components are missing. One can observe a standard depiction.

### 3.8.1 Hydra

Hydra is a parallelized login cracker that can attack many protocols. It is really quick and adaptable, and adding additional modules is simple. Researchers and security experts can demonstrate how simple it would be to obtain unauthorized remote access to a system with the help of this tool. is a flexible and strong command-line utility made to carry out online password attacks on different remote services. It is a versatile and adaptable dictionary- and brute-force password cracking tool that works with a variety of protocols and services. Hydra's main goal is to try to get past password defenses in order to test the security of networks and systems.

The strength of Hydra resides in its capacity to launch dictionary and brute-force attacks against a variety of protocols and services, such as but not restricted to:

Secure Shell (SSH)

File Transfer Protocol, or FTP

Telnet HTTP (both Digest and Basic Authentication)

Server Message Block, or SMB,

Remote Desktop Protocol, or RDP

The email protocols POP3 and IMAP

PostgreSQL, MySQL, and more database system

You'll need to supply specifics like the target host, protocol, and usernames (for certain attacks) in order to use Hydra efficiently. By providing character sets, password dictionaries, and other parameters, you can further personalize the assault. As a powerful and adaptable password-cracking tool, Hydra Linux has gained recognition for being a crucial part of security testing and ethical hacking. It offers important insights into the security posture of systems and networks due to its capacity to evaluate password strength and find vulnerabilities in a variety of protocols and services. But when utilizing technologies like Hydra, it's important to keep in mind that responsible usage, appropriate authorization, and adherence to legal and ethical requirements are non-negotiable. Hydra may be a tremendous ally in the continuous fight to defend our digital world if the right policies are followed and the appropriate safeguards are taken.

## SQL Map

In essence, it is merely a tool to simplify SQL Injection. According to their official website, SQL map is an open-source penetration testing tool that makes it easier to find and take advantage of SQL injection vulnerabilities and take control of database servers. It has an effective detection engine, a ton of specialized features for the ultimate penetration tester, and a wide range of switches that cover everything from database fingerprinting to data retrieval from databases, to gaining access to the underlying file system and running operating system commands through out-of-band connections. The main feature on the SQL Map website is "full support for database management with MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, and SAP MaxDB. Basically all the database management systems. Most of the time you'll never come across anything other than MySQL (mohammed, 2024).

It provides a list of the fundamental commands that SQL Map may support. First, we will run the following short command: `SQL map -u <URL to inject>`. In this instance, it will be

SQLmap -u Listproducts.php at <http://testphp.vulnweb.com> with cat=1

Using the `-time-sec` option can occasionally help to accelerate the procedure, particularly in cases when server responses are sluggish.

```
SQL map -u -time-sec 15 http://testphp.vulnweb.com/listproducts.php?cat=1
```

Upon completion of SQL map, you will be able to see the My SQL version and other helpful details about the database.

### 3.8.2 John the Ripper



Figure 9: logo of john the ripper tool

The Open wall Project created John the Ripper, a popular open-source password cracking program. Although it was initially developed for the UNIX operating system, it is currently accessible on a number of platforms, such as Windows and macOS. John the Ripper is a useful tool for security professionals and penetration testers because of its reputation for cracking passwords, even those that have been hashed or encrypted.

Network traffic captures, encrypted private keys, and user passwords from different operating systems are just a few of the password forms that John the Ripper can handle. Its automatic encryption detection for popular formats and its instantaneous hash generation for dictionary passwords make it an effective and multipurpose tool for password cracking.

**Dictionary attacks:** Using a wordlist of possible passwords, John the Ripper is able to carry out dictionary assaults. This technique works well for breaking weak, popular passwords.

**Brute-force Attacks:** In order to find the correct password, the program also supports brute-force attacks, which involve methodically trying every conceivable combination. This method is effective for cracking complex passwords, despite its time-consuming nature.

**Password Hash Algorithms:** MD5, SHA-1, SHA-256, and other hash algorithms are just a few of the many password hash methods that John the Ripper supports. Because of its adaptability, it can decipher passwords encoded in a variety of cryptographic formats.

**Customizable Cracking Rules:** Users are able to fine-tune their password cracking attacks by creating custom rules that take into account particular patterns or attributes of the target credentials (mohammed, 2024).

The Rainbow Table Attack is a sophisticated technique that expedites the password cracking process by utilizing pre-computed tables, sometimes known as rainbow tables.

In essence, rainbow tables are huge databases that include pre-calculated hashes of potential password combinations. They are less successful, though, against systems that "salt" passwords—that is, add random data to them before hashing.

When it comes to cybersecurity, password cracking programs like John the Ripper can be very useful in determining how secure a system is. However, it is important to stress that these kinds of operations must be carried out in the strictest legal and ethical manner possible. Those that use password cracking software should be careful to follow rigorous ethical guidelines and make sure that their acts are done with permission (mohammed, 2024) . The use of instruments such as John the Ripper without authorization or legal justification is strictly forbidden and may result in harsh legal repercussions.

Essentially, John the Ripper functions as a versatile instrument, utilizing an array of attack modes, customization choices, and user-specified parameters to methodically examine and decipher password hashes. Because of its versatility, penetration testers and cybersecurity experts who want to assess how reliable authentication systems are tend to choose it. But it's important to stress that using John the Ripper responsibly and with authorization is essential since, if used unethically, its powers could seriously jeopardize user privacy and system security.

#### 4 CONCLUSION

- Kali Linux is a Linux distribution intended for penetration testing and digital forensics. Offensive Security provides funding and maintenance for it. For both experts and enthusiasts in cybersecurity, Kali Linux is a powerful tool. It is a vital tool in the fields of digital forensics and ethical hacking because of its extensive toolkit, long history, and security-focused approach. And its importance can be felt and realized by organization and individuals in what it provide for them. For

me kali linux is incredible and it can be shield and give people a sense of security about their information and belongings.

- Kali Linux is an operating system that may be installed on any type of hardware. Installing the platform is a useful alternative as it offers additional tool combination options. It can be installed or used with any Linux and Windows operating system. Upon accessing the website, a variety of platforms can be downloaded. The installation can take time depending on the internet speed you have. It is not a tedious process rather is straight forward in that it does not require a lot and it does not take much to install Kali Linux.
- Guidelines are typically needed for any activity involving ethical hacking, penetration testing, or security assessment. These may or may not contain every target, but they usually don't. You have to choose your objectives while keeping in mind human aspirations as well as systemic ones. To do that, you'll need to engage in what's referred to as reconnaissance. Attacks can target not only systems and the programs that run on them, but also specific humans.
- A lot of individuals could confuse penetration testing, which aims to increase privileges by gaining access to systems, with security testing. Experts, and certification agencies in particular, always bring up the "triumphero" when talking about security. Information security is unique because of its three pillars: confidentiality, integrity, and availability. Anything that could have an impact on any one of these characteristics has an impact on the security of any software or system.

## 5 Bibliography

Boteanu, D. (2011). Penetration Testing: Hacking Made Ethical to Test System Security. *Canadian Institute Of Management*, 10-11.

Fletcher, S. (2019). *Hacking with Kali linux*. Publisher Association And American Bar Association.

hoffman, h. (2020). *ethical hacking with Kali Linux*. American Bar association.

kali Linux . (n.d.). *Get Kali*. Retrieved from Kali Linux: [www.kali.org](http://www.kali.org)

Messier, R. (2018). *Learning Kali Linux*. O'Reilly Media, Inc.

mohammed. (2024, January 5). *Medium*. Retrieved from Medium: [www.medium.com](http://www.medium.com)

Tutorial point. (2018). *tutorial point*. Retrieved from tutorialpoint:  
<http://www.tutorialpoint.com>



Atlantic International University

*A New Age for Distance Learning*

