Ethical Hacking & Cyber Security (CEH-V11)

This internship report submitted in partial fulfilment of the requirement for the award of degree

of

BACHELOR OF TECHNOLOGY

in

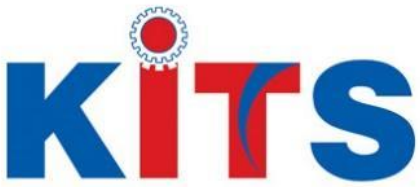
INFORMATION TECHNOLOGY

by

21JR5A1204

Under the esteemed Guidance of

Mr. Aluri Bindu Sagar.



KKR AND KSR INSTITUTE OF TECHNOLOGY AND SCIENCES

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

KKR & KSR INSTITUTE OF TECHNOLOGY AND SCIENCES

KITS -- GUNTUR

(Est. u/s 3 of UGC act 1956 & Accredited by NAAC with A+ Grade)

GUNTUR -- 522017

2020-2021

Declaration

I **BANDARU JAYA VENKATA SAI MANIKANTA,** student of III YEAR 1 Semester B.Tech in the department **INFORMATION TECHNOLOGY**, declare that the internship entitled (Ethical Hacking & Cyber Security CEH-V11) has been carried out by me in Supraja Technologies Guntur during ……, 2022 to ……., 2022 This report is being submitted for the fulfilment of my internship and for record purposes.

Place: **Guntur**

Signature

Date:**……,2022.**

Employee ID: **ST#IS#3235** _____

ACKNOWLEDGEMENTS

With great solemnity and sincerity, I offer my profuse thanks to KKR KSR INSTITUTE OF TECHNOLOGY AND SCIENCES management for providing all the resources to complete our Internship successfully.

I am extremely grateful to my Technical specialist Mr. Santosh Chaluvadi, I wish to express my whole hearted gratitude to my Internship guide Mr. N. Mahesh Chowdary,

Special Thanks to Supraja Technologies Team who has given me inspiration and encouragement throughout internship.

I Owe particular debt of gratitude to Prof ……, Head of Department of INFORMATION TECHNOLOGY for providing all facilities required for the internship.

I thank Prof. Dr. P. BABU, Principal, KITS, for extending his outmost support and cooperation in providing all the provisions for the successful completion of the project.

Regards,

_

ABSTRACT

In this Internship, we learn about Ethical Hacking and Cyber Security. The ethical hacking teaches you all the information about the networking world. It also teaches all the ways to attack a system or any company. But here we must learn all the methods to secure our website from the attacks caused by the penetrators or hackers. They are too dangerous for any company or system.

The Ethical hacking is fully a legal way, if we could do it in a perfect way without errors. The ethical hacking helps us learn to think in the attacker way and protect our system by giving protective measures from those attacks estimated.

The Cyber Security comes under the protective methods giving for securing a website or a company. This is the only way to secure a website from the attackers and hackers.

We learn the very basics to the extreme level of using the hacking tools and techniques. We also gain total knowledge about the ethical hacking in this evolving networking world.

All this knowledge is useful in protecting our selves or our company and even to educate our surrounding people with minimal knowledge to secure themselves and beware of the scams in this Electronic Era.

INTRODUCTION

Hacking: Hacking is finding a small entry point that is already present in a computer software or network and entering into them. Hacking is especially done to gain access of the system without knowing to the original user or target. Hacking is done to gain even the sensible information of the target or the user to gain profit financially in direct manner by pretending to leak the information or by other sources like selling the data of the user to the people who need that sensible information.

"Hacking", this is not a new term or process invented just in the 21st century. This had taken place first at MIT, in 1960. The terms 'Hacking' and 'Hacker' are termed at the time it took place itself. A Person who does 'Hacking' is called "Hacker".

Hacker: Hackers are those who learn the knowledge to understand how the computer software or network controls operate and also learn the deep knowledge about the blueprints of the systems and processes. Then they attempt to interrupt these systems and gain the information.

There are Different types of Hacking Processes. We distinguish them into types based on the process carried out and based on which information is being leaked:

- **Computer Hacking:** In this process, the computer ID and password are being hacked and the unauthorized access is gained. The data in that computer or PC is stolen.
- **Password Hacking:** This process is that in which the secret passwords hidden in the information that is stored or being transferred by a system or software.
- **Website Hacking:** Website Hacking is that gaining the admin control of the website or it's server and the linked software, data collections and other linked devices.

- **Network Hacking:** Network Hacking means knowing all the knowledge and information of the network that is targeted by using tools to gather the information. And by knowing the open ports present in the network to destroy the network and demolish the devices connected to it.
- **Email Hacking:** It is hacking the targeted Email account and unauthorized usage is done.

These are quite dangerous which results in:

- Security Breach

- Unauthorized Access to Sensitive Information.

- Privacy Interruption.
- Malware Attacks on the systems.

Possible reasons for Hacking:

- Masochistic Fun.
- To tell everyone that he can do it.

- Financial profit.
- Damage the opponent's system to make him loose his wealth.

Just like the coin having both sides, here there is another type of hacking for good deeds.

There is a way to find the threats to our system, that is **'Ethical Hacking'.**

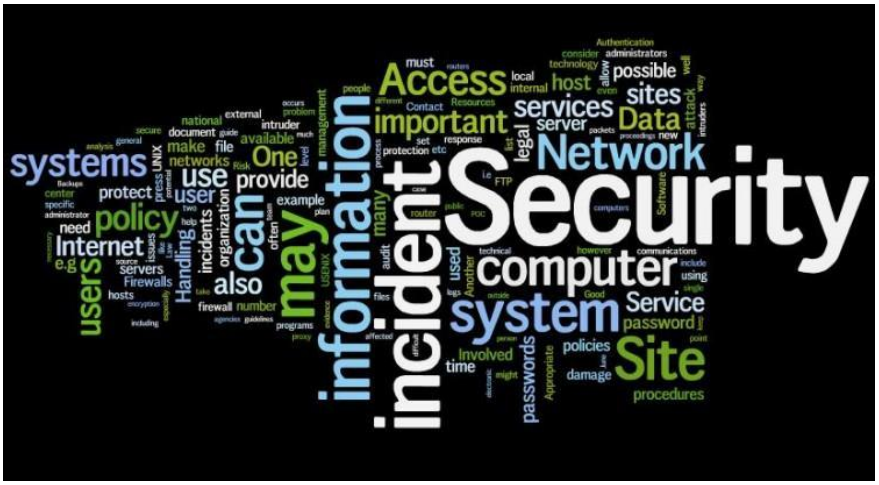
Introduction to Ethical Hacking

The process involved in ethical hacking is same as hacking, the only difference is that, here we find the entry points or weak targets for getting them fixed.

Ethical Hacking: Ethical Hacking is finding the loopholes present in a system or software for getting them fixed and loops free system to secure it from threats and hackers. The one who does it is called "Ethical Hacker". This involves the knowledge of hacking and finding the ways that a hacker could use to affect our system and trying to protect the system in defending those ways.

Ethical Hacking is indeed a Good way to protect our system or website, the name itself says 'Ethical'(Good). Simple policy "To defend the attackers, we need to think in the same way". To protect our system, we should think in all possible ways that an attacker can attack our system and protect it in all those ways.

Here, there are rules to be followed and changed from a company to company and system to system. Ethical hacker finds utmost ways to attack our system and ensures that those ways are being protected.



To first get into Ethical hacking, we need to know about some words that are very essential in further understanding:

- Vulnerability – Weakness.
- Exploiting – Attack caused due to Vulnerability.
- Payload – Using the Vulnerability.
- Bug – The odd one or the mistake in the code of the system.

There are some types in the vulnerabilities even:

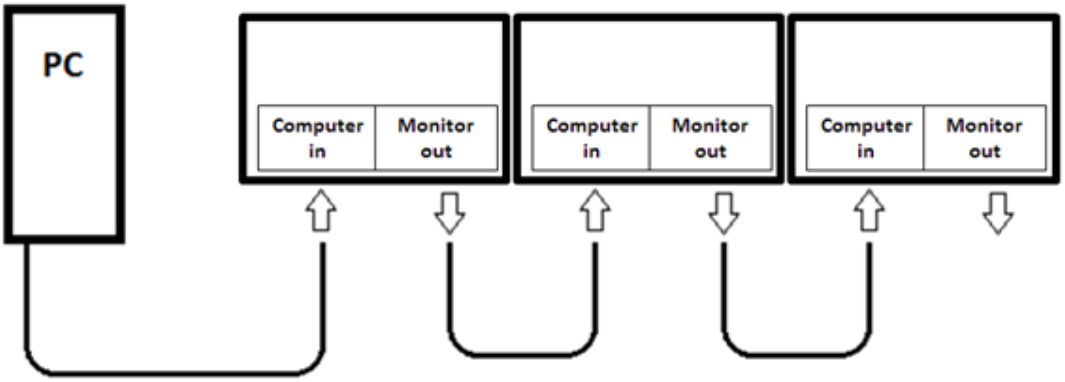
1. **zero-day Vulnerability:** It is that the vulnerability is found within the starting days of the release of the app/website/system but not covered it or patched up. “Zero-Day Exploit” is that the exploit which attacks the zero-day vulnerability before patching it up. Vulnerable systems/apps/websites can be easily exploited until they are being patched.

2. **n-day Vulnerability:** The vulnerability which is not patched up even after a no. of days after knowing the vulnerability by the developer. The "n-day vulnerability attack" is that the attack on the vulnerability that is not patched up even after knowing about it.

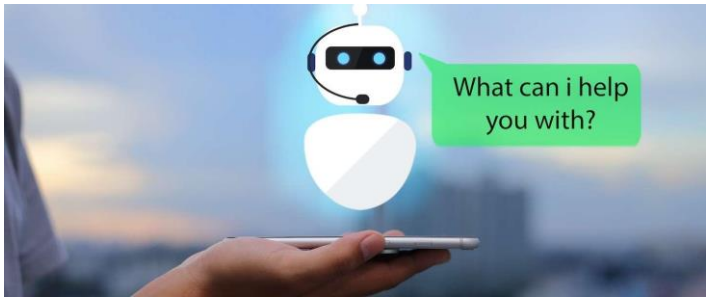
Some unknown terms:

1. **Doxing:** It is sharing the information in public which is obtained from hacking someone's system. It is knowing a person's data which may be very confidential to them and keeping it in public.

2. **Daisy Chaining:** It is like a series connection of the electronic devices or systems like a chain, through which hacking is possible from one system to the other. This is used to hide the original info of the person hacking the data.



3. **Hack Value:** It is nothing but the value of the hack we are ought to do. Hack value is checking whether the expected data through hacks is worthy of hacking it.
4. **Bot:** Bot is an Artificial Intelligence running software that is programmed to do some specific tasks automatically. For example, we get some automatic replies in some websites, they are called chat bots.



Phases of Ethical Hacking:

There are many phases in ethical hacking, in fact these are the steps involved in this ethical hacking process.

1. Reconnaissance.
2. Scanning.
3. Gaining Access.
4. Maintaining Access.
5. Clearing Tracks.
6. Reporting.

NOTE: Hacking is considered illegal, these are followed only for the whole purpose of ‘Security’.

1. **Reconnaissance:** Firstly, we need to collect all the required information of the target system, by having a little survey at least. Observe all the information collected and keep an eye on the target at different times for different type of requests. It involves unauthorized discovering of the target to collect information about vulnerabilities.

2. **Scanning:** Scanning Comprises of some sets of processes to find the information about vulnerabilities like knowing all the ports in the network connected to the target, knowing about the operating system used by the target and other services involved. Specific or sets of tools are used to know the vulnerabilities in the target based on the target type.

3. **Gaining Access:** With all the information got, and knowing about the vulnerability, we should gain access to the target with the help of this vulnerability. The tools used must be of safe and secure that shouldn't damage our system and the target system.

4. **Maintaining Access:** The access got through the vulnerability must be maintained confidentially and shouldn't disturb the processes in the target system. Silently use this without knowing to the target user.

5. **Clearing Tracks:** Before leaving the target, we must make sure that the logs we made must be cleared, not leaving any small clue to make the host know that we entered the system. The same path must be maintained while coming out and shouldn't use any other tools, Clear the path without footprints.
6. **Reporting:** As an Ethical hacker, to make a difference between a hacker and ethical hacker, we must report all the processes and information we got. The main aim of our entry to the target and the vulnerability we found, everything must be reported to the host company that appointed us to find bugs.

- **Bug Bounty:** Bug bounty is nothing but, the bounty(money) is paid by the companies for finding the bugs in their software/code. This is done with the prior information given to the company.

- ***Including ethical hackers, there are many types of hackers along.***

Hacker Types:

With the growing world of technology, in just a span of 2 decades, we evolved from registers, ledgers, paper files, documents to computers. Every field is somehow related to computer these days. All our data which is need to be stored either confidential or public data, everything is stored in the computer. This data can be stolen easily with this computerization, if there is no proper security. This is somehow found profitable to some people with bad intentions and then based on the type of hacking they do; they are divided into various types:

These are the main types of hackers in the world of networks, they are of different knowledge, equipment. They differ in many things but we consider the goal/moto of them to divide them into categories. These are only some of the types of hackers, out of these the most important hackers are shown like: Black, White, Gray Hats.

1. **White Hat Hackers:** White Hat Hackers are those who are proficient in this skill and are certified and authorized to hack any system. These are the people called ethical hackers. They are well certified with best knowledge from the EC-Council and are appointed by organization in order to help them secure their websites or systems from hackers and keep their systems vulnerable free. They hack the systems with the vulnerabilities present and test the cyber-security level of the system and ten find patches for those vulnerabilities.

White Hat Hackers work as per the rules and policies of the company, they are the whole and sole responsible for any security related issue of the company system/server. They either get the confined salary or given based on their work for the bugs they found and patching them up. The main goal of these white hats is protecting the company or the organization.
They help the companies grow their business and Circle; they help them to create a defence system to protect against the cyberattacks from the hackers. They detect the vulnerabilities and patch them up before the hackers find it. They report their entire work to the company who appointed them. This is the main reason where the hackers are separated from ethical hackers.

2. **Black Hat Hackers:** These are considered as unauthorized hackers they won't follow any rules and policies. They just do anything they want with their knowledge but keep their identity secret. They damage any system they want to and get the confidential data if the target system is vulnerable even at one point. Most of them do this for money or other profits, some do it for Masochistic satisfaction and for fun. Some do to damage the opponent's wealth. They are very skilled and knowledgeable; they have all the resources and gather all the information by anu basis to destroy the target. They are very much skilled, highly equipped but are with wrong intention.

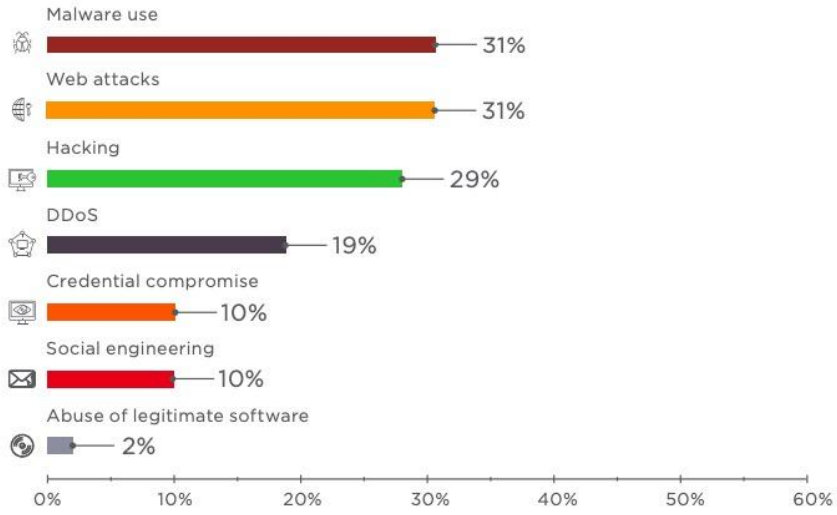


fig: Various types of attacks done by a black hat hacker on an average per year.

It is very difficult to find them and their location. As they are well equipped to hack and also hide themselves.
The hacking range depends on the amount of data they want to steal and the profit they get by selling that data. Sometimes these are hired by reputed organization to attack on the opponents, to damage their wealth and data.
The Black hat hackers, don't have a specific reason sometimes, they just want some fun and to make others know that they exist and frighten them with their works. They even send anonymous messages on the screens of the users in order to terror them. No other application would work at the time they take control over the systems, except the thing the hacker wanted to show us. They hack into organizations and steal the data and resources; they use these stolen data to earn money. They keep this data in dark web and black market to blackmail the target company.

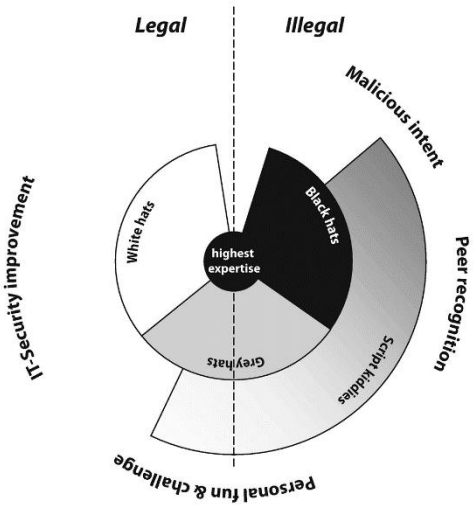


fig: The systematical difference between white and black hats.

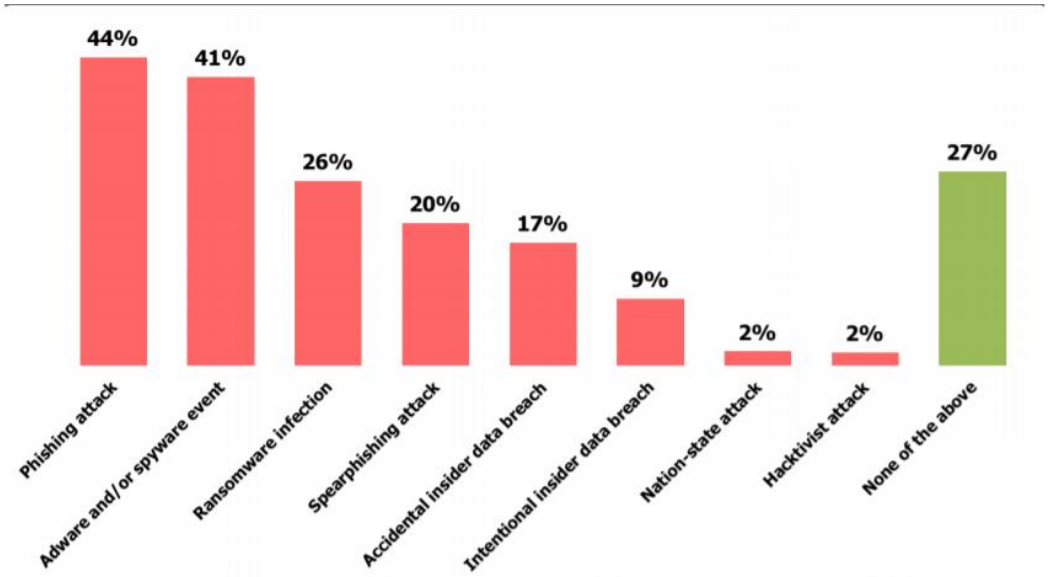


fig: This shows different types of attacks that are done on average per year.

3. **Gray Hat Hackers:** These types of hackers fall between white hat and black hat hackers. They are not well certified hackers; they don't have neither good or bad intentions. They just do it to gain some profit for their needs and sometime for fun to test their knowledge extent. They don't want to steal or rob money from people. They just try for the vulnerabilities and loopholes of some random sites not targetable and get some data to sell it to the people who might need it with bad or good intentions. His goal is only for personal profit for his supper and not target anyone. They don't want to steal people money or data neither they want to help people. They just do it most of the times for fun and test their

hacking knowledge, as a result, if they get any outputs, they sell that in the black market or web. They can be found if concentrated on them.
These are the most important hacker types in the network to know about them.

There are few more types:

4. **Green Hat Hackers:** Green Hat Hackers are those who are looking for opportunities to learn from well qualified and experienced hackers. They look for the chances to learn and gain knowledge from the acts done by well learnt hackers. Their main goal/moto is to become a professional or perfect hacker by learning and sometimes they try to use the tools and learn. Their intention is not to damage anyone or gain profit but sometimes it may happen while learning. They won't cause much damage to anyone as they don't have any targets. After gaining some knowledge, they try their knowledge on the websites or systems of other countries which do not cause any damage/ problem to them. They are not even well-equipped to do professional hacking that may affect someone else. Even if they cause any damage, it is very easy to find them and warn by knowing their intention.

5. **Red Hat Hackers:** Red Hat Hackers are those who are professional hackers and are ethical hackers same as white hat hackers. But their dealing with the attackers is different. White hat hackers provide security to the company/organization's system. But these red hat hackers deal in a rude way with the attackers. After finding the hacker who is attacking, red hats attack them back with mor powerful tools to damage the hacker's systems and equipment.

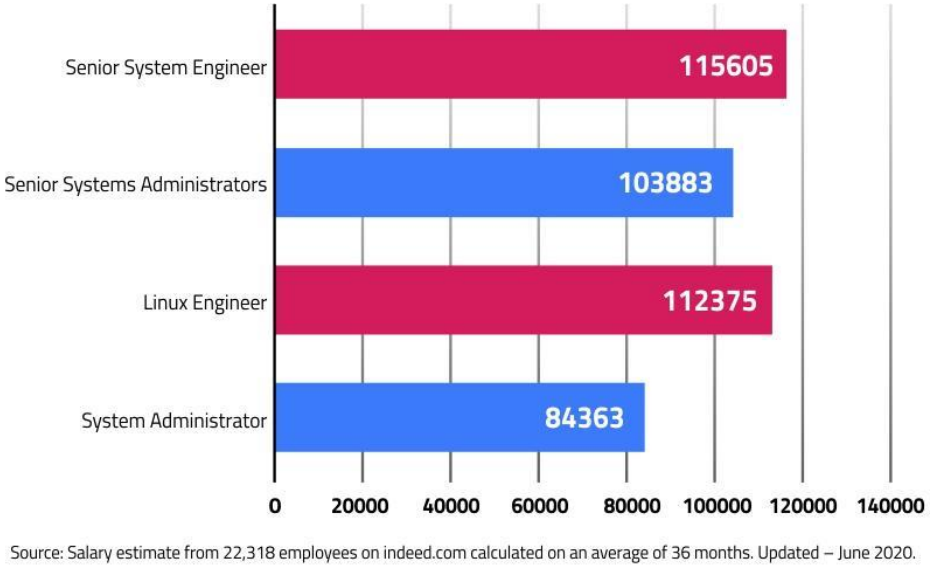


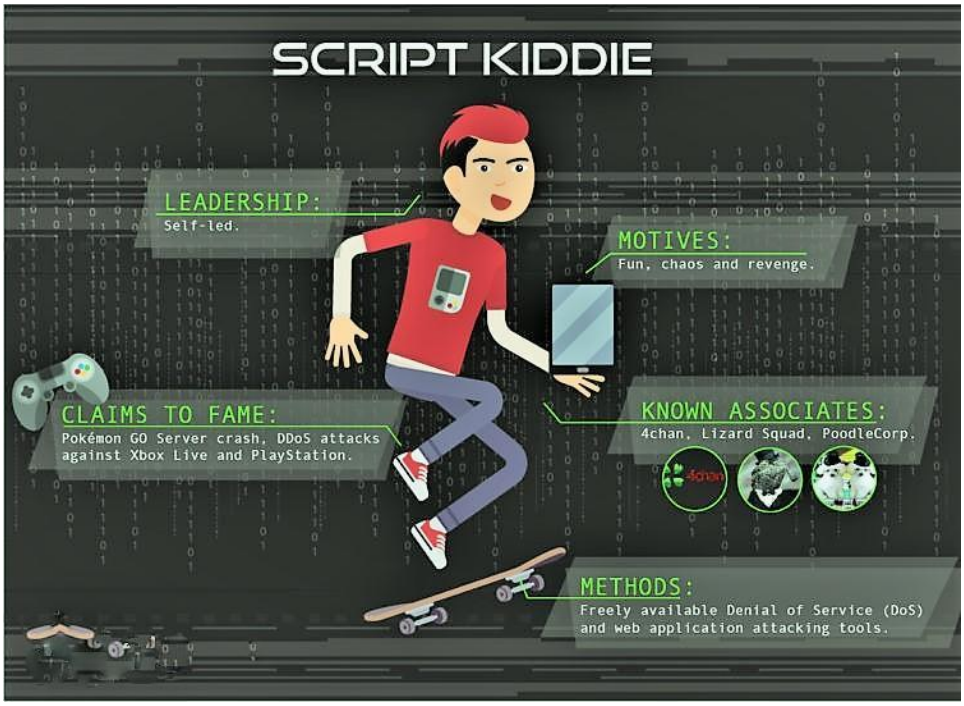
fig: Graph showing average income of the red hat hackers (Survey).

Their attacks on the hacker may even damage the host system as the same load is on this system too. There may be loss financially for both hacker and the host too. Their intention is to damage the system of the hackers that are attacking on the company's system. But it results in loss for the company that can even make a chance to replace all the host systems with new ones. They use brutal malwares to attack the black hat hackers that even damage the hardware of the attacker with the load. These are also appointed by the companies as ethical hackers. Their intention is also to stop the Black Hat Hackers. There is demand in the market for white hat hackers and red hat hackers. Compared to normal developers, red hat developers are preferred more in the market; they are paid more salary too.

6. **Blue Hat Hackers:** Blue Hat Hackers are those who don't have much knowledge on hacking but do it by knowing about some tools and their usage. They do not think about the consequences and results of the work they do. They do it for show-off at their friends. The moto to learn the knowledge about it is not seen. They do it even for gaining popularity among their peers. They even do it to solve small problems of their friends or themselves like spying on someone by hacking their social accounts to check whether the person is genuine and to know their secrets.
   They specifically don't have any intention to attack someone but have the wrong intention. They don't look for any profit in data or money. They just use hacking for settling their disputes with their enemies in their student life/job life.

Apart from these, there are some types which not so much important but to be known:

7. **Script Kiddies:** These are just the people with low knowledge or half knowledge people. That is always dangerous to them. They just learn some hacking tricks from the internet like Google, Youtube and others. They just follow the set of steps shown there. They don't even know how much it results-in. The intention behind it is getting fame among fellow peers to show them that they could hack some sort of things like wi-fi passwords. They sometimes find misleading tools on the web and use them. This may lead them to fall in trouble. They just select a random site or system and use those tools on it. They just don't care the range of the company as they don't have the knowledge about it, they found it randomly.



8. **State or Nation Sponsored Hackers:** These are the hackers that are hired and appointed by the government for helping them to find the secret information from other countries. To know their plans and blue prints of attacks. By knowing this, they can protect the country from those attacks. They even want to know the confidential secrets of other countries with the help of these hackers. They are utmost trained and lots of knowledge about hacking.

They even warn the governments about the upcoming attacks on them to be prepared for it. It is mostly used in military purpose.
They use their knowledge to help the governments by gaining the information of other countries through their loopholes in the data devices. They eve attack them without even having a trace of who hacked and even the location of this hacker can't be found easily. There are many statistics about these hackers and the information collected by them. Many a times, they helped in stopping major attacks physically and even the cyberattacks. They provide a strong security layer that no one can penetrate into it, almost all countries with some high resources do the same with their government related works. These Nation sponsored hackers directly report to the government and are not answerable to any others.

9. **Hacktivists:** These hacktivists are totally different from any other hackers. They say themselves as hacktivists. They have complete knowledge in hacking, but they intend to hack only the websites of the government related portals. They gain access over these websites and know all the data related to public.

They do it not for profits, they do it to show their agitation over the bills passed by the government. They try to change the information in the websites to mislead the government. The data gained by the confidential information is used for political gain by the opposition parties and sometimes used even to bring a movement in people in opposition to the bills or GOs issued.
There are many companies sometimes effected by hacktivism. The employees or the common people who can't tolerate the decisions made by the company could even hack those systems or websites. They take the help of some whistle blowers and educate people regarding the depth in the company's decision. They bring a movement in the people and make them fight against it.

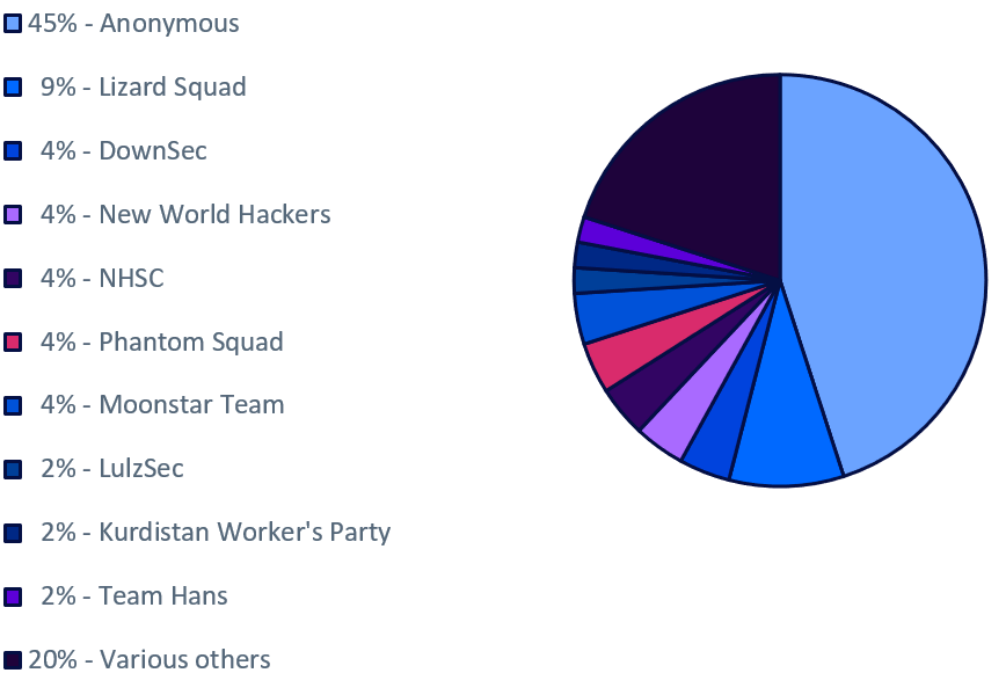


fig: The figure shows some hacktivist groups that caused the attacks on governments worldwide.

The Squads shown above are different types of hacktivists groups. They attacked many government sites when there are bills passed which are opposite to the benefits of common people. So, most of them get support by common people and they are not that easy to be found as they have people support. Most of the hacktivists show their protest using a mask as shown below:

This mask is also used by the people in support of the hacktivists and their works. They just bring movement in people and help them fight for themselves and they don't need any profits.

There are some more types of hackers which are typical ones; they are said as follows:

These involve some of them like blowers, newbies, cyber terrorist, suicide hacker, elite hacker, etc;

1. **Whistle Blowers:** The Whistle blowers or Malicious insider are those who are appointed by the company themselves. But they leak the information to the other companies or to the people who may be profitable with the information of this company. They do this because of some personal grudge or anger on the company. The intention of this may be anything. They be in this company and leak the confidential matters to the opposite people. This may even happen when there may be some bad or illegal activities happening in the company; to bring out those, they may leak the information and stop it to happen.
   The reasons may be different but the intention in the view of the company is wrong. So, they are called whistle blowers.

2. **Suicide Hackers:** This type of hackers does dangerous hacking that destroy the other systems. But they don't care about the consequences, even though they know about the issues he may face. They don't care about their lives even. So, they are called suicide hackers. They just do this for mainly some reasons like demanding lot of money or to take revenge in the bigger enemies of them. This is suicide hacking because, they know that the police would definitely catch him. They also do it for third parties by asking them to take care of their family for life or give a lot of money for them after the mission. They just don't care about the consequences and the police. Hey are prepared that they would be caught and put in the jail but they work for the money they get.

3. **Cyber Terrorists:** They are the hackers who hack the system or websites using the vulnerabilities and gain access. With this access, they create fear among the people who use those websites or systems. Just like putting anonymous faces and sounds that appear suddenly which may make some people afraid.

They even show some murder scenes which may fear the people who are using that system at the time. These are mainly used by the terrorist camps to bring fear among people of other country.
They have the intension to fear the people and earn satisfaction. This acts also involves mental torture to the targeted people. They even make some offers to the people who may be weak, to join their terrorist groups and help them in malicious activities in the user's country.

They just use them as sleeper cells, they use them whenever they want. They offer money and luxurious lives to those people who are in their trap.

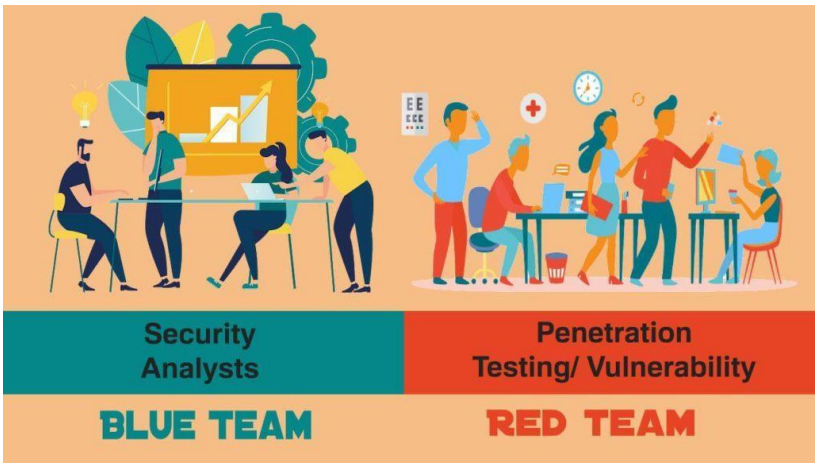
4. **Newbies:** The people who are new to the hacking are called newbies. They are ought to learn about hacking. They either learn from any training institute or take the ethical hacking courses from the internet by buying the premium of the courses available. They even buy the tools premium to use them in the hacking process while learning. This stage declares the person to become a professional ethical hacker or a knowledge less hacker. And the intentions caused here make them an ethical hacker or a black hat hacker.

5. **Elite Hackers:** Elite hackers are those who are well qualified and certified in higher level. They don't have any tie-ups with the companies or any other organization. They just concentrate on the vulnerabilities. They find them and report to the company to get money from them. They help the companies to protect them from attacks by finding the vulnerabilities. The Elite hackers have high-end technology with them and even high knowledge in hacking. They just mainly concentrate on single vulnerability most of the time. They can even

write their own exploits to enter into other systems of the opponents. They can easily enter into attacker's system with these exploits.

In many companies, there are only two teams always:

1. Red Team.
2. Blue Team.



1. **Red Team:** The Company owners or organization heads gives the red team all the details and software to find the vulnerabilities. Their work is just to find the vulnerabilities and report them. They try in all possible ways to find the vulnerabilities and report to the authorities if they find vulnerabilities. The red team consists of some of the most experienced hackers in the network. They are not only hackers but also penetration testers. They test these systems and websites. They just not only find vulnerabilities; they do black box testing, exploiting vulnerabilities and check the damage to be caused by that vulnerability. They even do penetration testing to check whether the system is weak to penetrate with malwares.

2. **Blue Team:** Blue team is given the vulnerabilities given by the red team. They find the security patches for those vulnerabilities. They analyse the malwares and attacks done and could be done on the system and create strong shields of security that can't allow the penetration of any malwares. They are defenders of the website/ system; After the completion of securing, they again send it to the red team to verify. Then they attack with all possible ways and if it is strong enough, the system is set for release. The blue team contains very high-end ethical hackers, they not only secure the website but also find the culprit if any penetration happens through the system. This is done digital forensics. Hey are the damage controllers of the system/website.

These are seen in most of the companies, but the bigger companies or MNCs they appoint some other teams along with these red and blue teams.

They are as follows:

1. Yellow Team.
2. Orange Team.
3. Green Team.
4. Purple Team.

1. **Yellow Team:** Yellow team are those who firstly build the software with their spectacular coding skills. They try their level best to give the code without errors and loopholes. They are the main reason for any application to be built. They are the 'Builders'.
   They actually are the people who do the work like code testing, developing, manual testing, results and verification.
2. **Orange Team:** The Orange team trains the developers regarding the cyber security and ethical hacking. They make sure that the written code is with the

inbuilding of the cyber security formats. They are people who train the developers to build. They even help them in building. They facilitate interaction and education.

3. **Green Team:** The Green team is the team which helps the company in reducing the cyber security cost. They totally try to reduce the cost of the expenditure spent on the cyber security. Because, mostly organizations spend most of the money on the cyber security but can't assure the security perfectly. They try to give perfect security for less cost. This is the team which brings cyber efficiency.

4. **Purple Team:** They are the team for facilitating improvements in detection and defence. They are there to sharpen the skills of red and blue team. They are very effective for spot checking systems in bigger organizations. Purple team is a security methodology where red and blue teams work closely to maximise cyber security capacity through continuously transferring inputs to the red and blue teams.

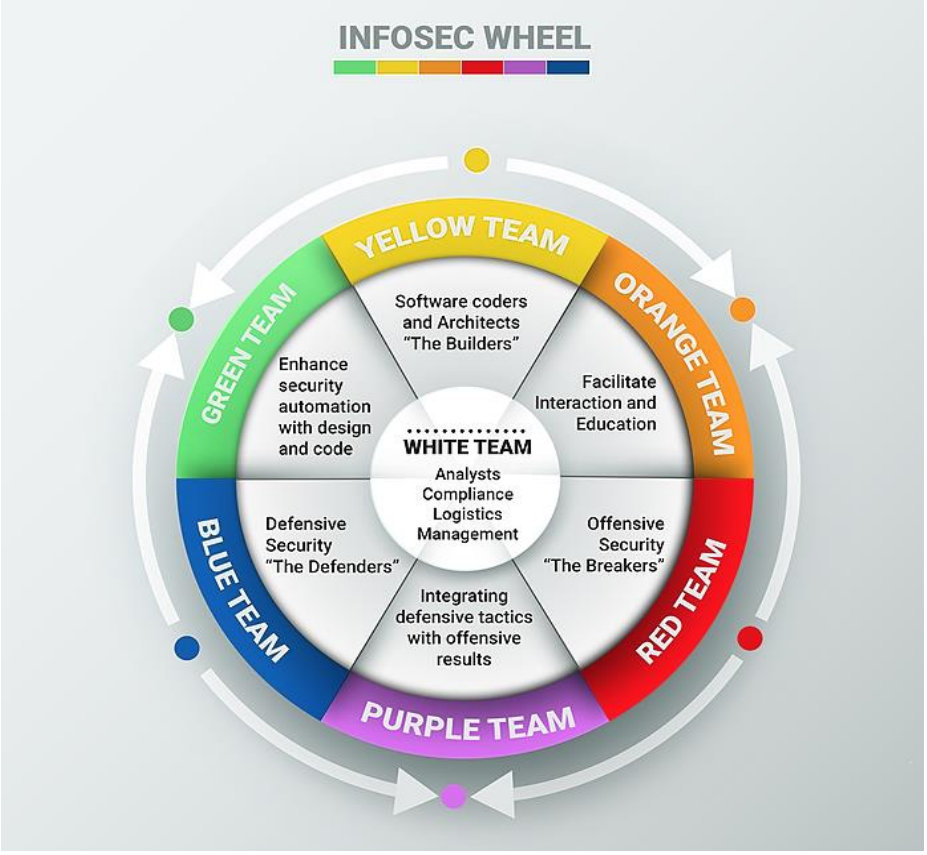


fig: This is called the INFOSEC wheel (Information Security wheel).

Now, let us talk about the cyber laws which are the main rules to be followed by ethical hackers in order to stay in the 'Ethical' way.

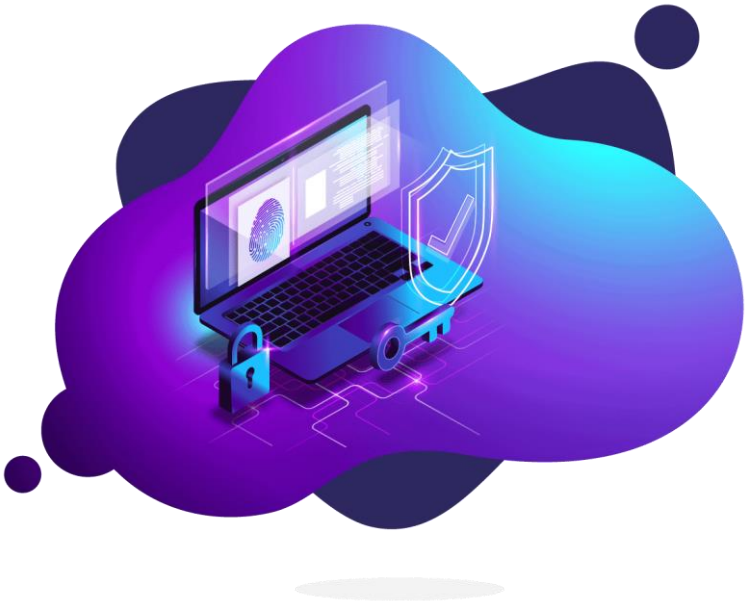
CYBER LAWS:

Before having brief discussion about the cyber laws, we need to know about the act that made these cyber laws. The acts are brought by the central government by passing it in the parliament.

Cyber laws are made to ensure a set of rules to make the difference between the correct path and wrong path in the cybersecurity and hacking. The cyber laws are those to make sure that there are wrong ways even in this network and used to stop them.

Just like the police department having IPC (Indian Penal Code), the cyber security also has an act called IT Act (Information Technology Act). The IPC Act is for physical crimes and this IT Act is for digital crimes/cybercrimes.

The IT Act came into force in the year 2000 by the Indian parliament on 9th June. It is introduced by Mr. Pramodh Mahajan, Ministry of Information Technology. It was signed by the former president Mr. K.R. Narayanan. The act comprised of all the cyber laws and later it was modified sometimes as per the need. There are many sections in the IT Act regarding the cyber-crimes caused. Before knowing those, let us know about Cybercrimes. The main aim of these IT Act is to secure the digital information and eradicate the crimes happening digitally.



CYBER CRIME: The criminal activities related to the computers and their security, data theft, damage, leakage of data, etc. All these come under cybercrimes. Majority of the cybercrimes are noted as frauds regarding money. The cybercrimes are not just easy to do and escape. There is high security eye on the cybercrimes. The cybercrimes are non-bailable. There is no bail in the law for cybercrimes.

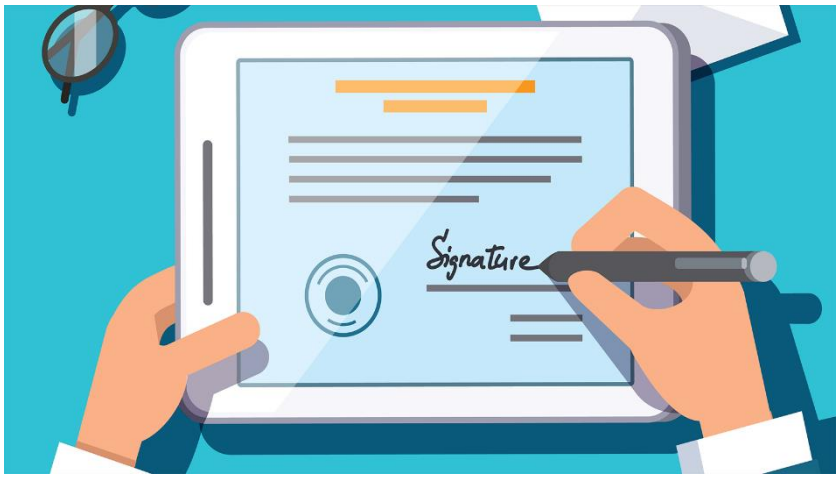
In this world of digital era, cybercrimes are getting common in the society. Main reason for the cybercrimes is, the criminals think they can't be identified as they are not putting out their real identity. The other reason for the increasing rate of the cybercrimes is people don't complain or care when they lose a small amount of money. This happens with lot of people, that funds the criminals in a large amount. With the increase in income, they commit more and more crimes, as they are not even struggling just with small work.

Let us know about some of the cyber laws in the IT Act to prevent the Cybercrimes in the digital world.

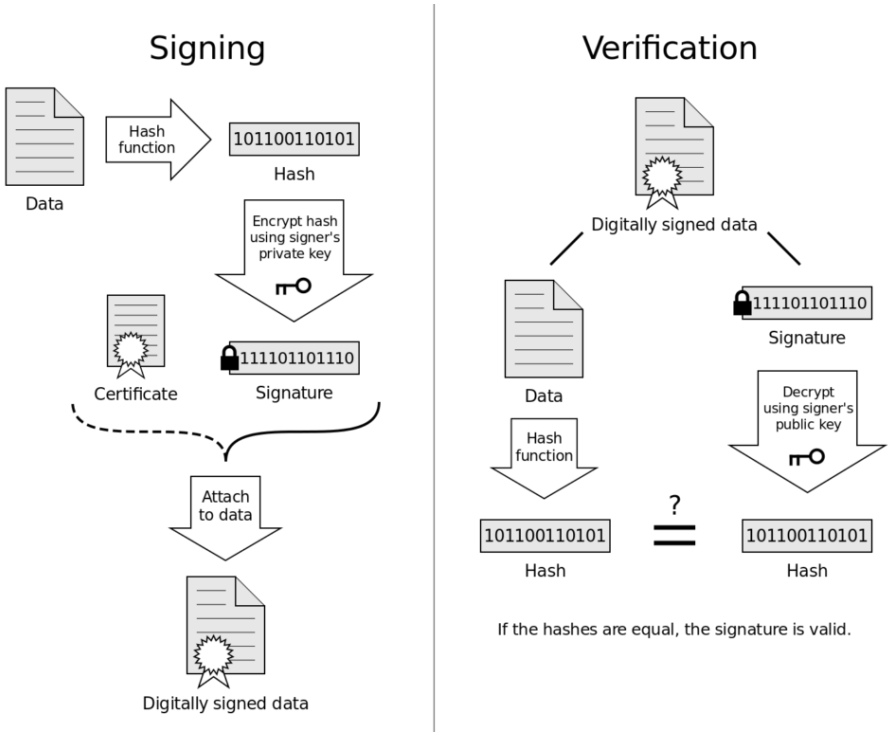
There are many sections regarding the cybercrimes in the IT Act. Most of them are against the Cybercrimes and other are about Cybersecurity. The IT Act has 13 chapters and 90 sections as per the current day.

From Section1(2) to section 75, there are a total of 90 sections. The main moto of the IT Act is to legalise all the digital network and transactions also. To prevent all the cybercrimes, it contains many acts and sections. It contains the clarified penalties to be imposed and the punishment to be given on different cybercrimes based on the impact they created. Some of them are like:

- **Section 3: (Authentication of electronic records)**
  (1): According to this section, any person or user can authenticate the digital electronic records by using a digital signature. Without the digital signature the data shouldn't be accessed. This can even be used as public key for others.



Subsection (2): The electronic data accessing must contain hash values that should be recorded. The electronic records must contain hash values even while transferring the data from one record to the another. So, even if the file is gone, we can recreate the file and its data with the hash values. All this happens with the help of the algorithm.

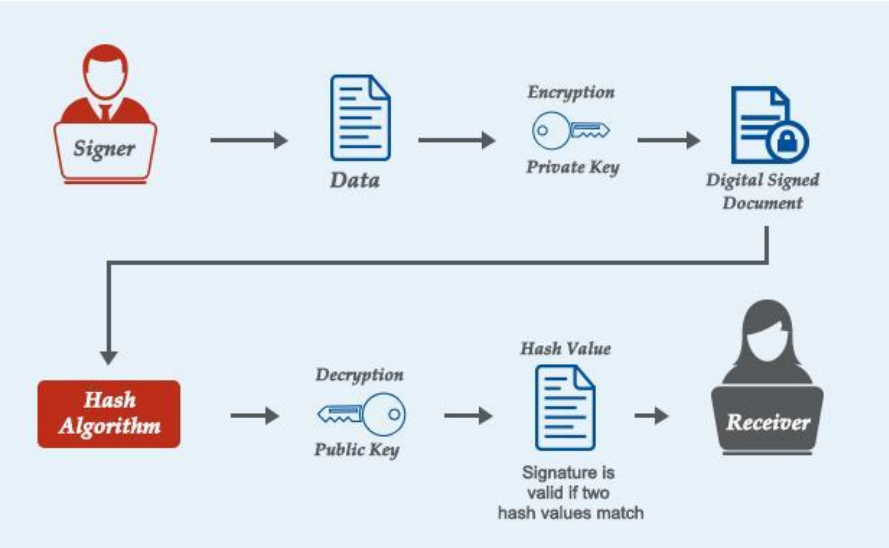


(3): The person using this public key can check the electronic records.
(4): The private key and public keys are different, but they are unique for every electronic documents. This is a unique pair for every electronic document.

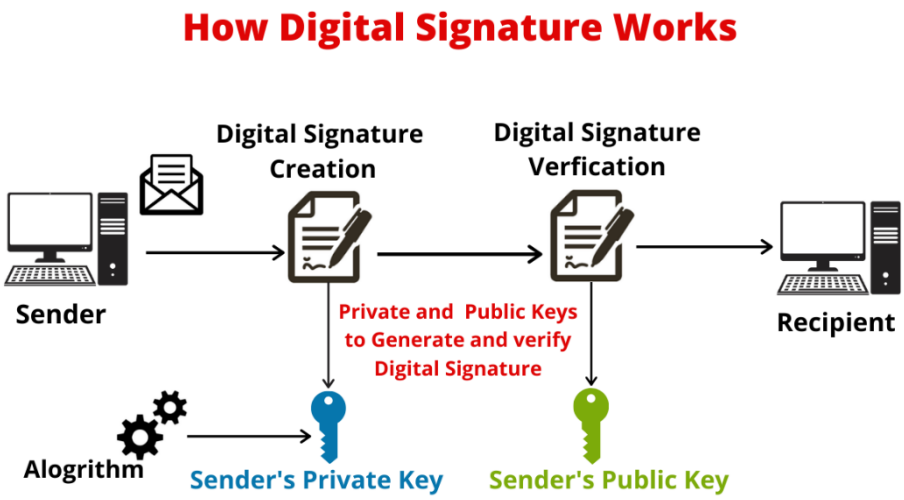
- **Section 3[A]: (Electronic signature):** The electronic signature contains the primary unique code or key given by the algorithm automatically when a file gets uploaded.
  (1): The electronic signature is considered reliable and trust worthy, if:
  The authentication data and electronic signature creation data are of the same person and not of another person.

(2): Any difference made in the data or record or n the authentication data to the time of creation is detectable by the user. The difference made in the data later

after the creation time is also detectable and should be noted by the hashes and algorithm.



(3): The central government may tell the purpose of this digital signature to the person who want to use the records at the start of the process.

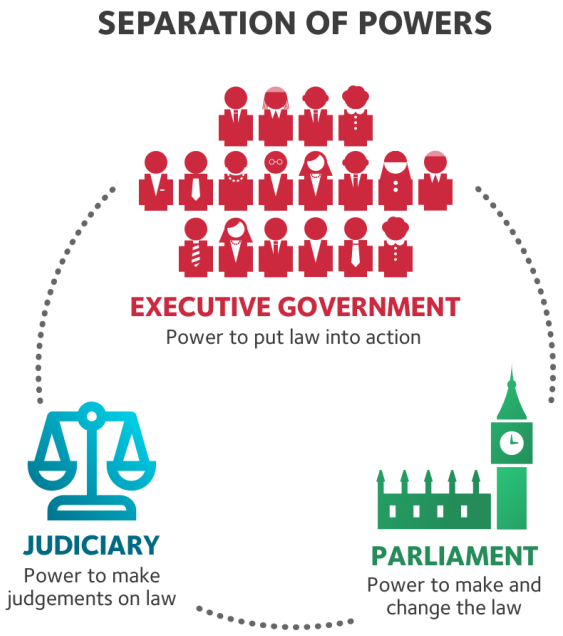


(4): The central government has the whole right to add or remove any technique which is essential for the electronic signatures with an official notification.
(5): Every section under these must be kept in the parliament as bills.

NOTE: There is a substantial difference between electronic signature and digital signature. The digital signature contains 2 factor-authentication with a seal to it with hash codes installed in it. Electronic signature is just a representation of uniqueness of the record, file, document or data we have to store or being stored.

- **Section 7A: (Audit for the documents electronically):**
  The documents that are kept electronically must be sent to an audit. This applies for the information stored, data, files, etc.

- **Section 10: (Power to make rules by the central government in parliament).**
  With the help of this section, there is chance for the central government to make any changes or bring new rules in the cyber laws. The whole power is by the central government that too with the help of parliament. The power is also divided into parts as shown below.



- **Section 40: (Generating key pair)**
  In any digital signature certificate, the public key of the corresponding private key must be listed in the digital certificate which is already accepted by the user/subscriber. The subscriber shall the pair of public and private key by using the security procedures which are different from system to system.
- **Section 40A:** According to this section, the user must perform all the duties in respect of the electronic signature.
- **Section 43: (Penalty for damage of computer, computer system):**
  If any person without the permission of the owner, or anyone who is the handling person of the computer:
  (a): access or secure the authentication without knowing to the owner, accessing the computer system, network;
  (b): downloads, extracts any data from that computer which is stored as data.
  (c): installs or cause of installing any virus to the computer system or network.
  (d): causes any damage to the computer, computer system or computer network. Causing damage to the data in the computer network, computer or computer system.
  (e): disrupts or causes disruption of any computer.
  (f): denies or causes the denial of authentication to any person who is the authorized user of that computer system or computer network.
  (g): provides help to a person who is the trails of gaining access to the computer or computer system.
  (h): destroys any data in the computer or modifying it which leads to the loss of original data.

(i): theft, steal or destroy or helps/assists any person who want to steal the data with an intention to destroy it or copy it.
With all these intentions above, the person who is responsible for those claimed by the user, must pay the penalty which is equal to the theft from him. The culprit must pay the compensation to the owner affected. ***(Not exceeding 1 crore penalty and 3 years of jail as punishment).***

- **Section 43A: (Compensation for failure of protecting the data)**
  If the person or group who is appointed for taking responsibility for protecting the information or data regarding to confidential ones, failed in protecting it. Like he failed in giving security to that data and information, then the person or that cyber security analyst is responsible for it and he is subjected to compensate the damage caused due to his negligence or his less knowledge. If this caused the company the unnecessary loss or gain to other person who attacked it due to the security group not taking necessary security patches for the vulnerabilities. **(Penalty of not exceeding 5 crores or punishment of 3 years of jail).**

- **Section 44: (Compensation for failure to furnish, protect information, return data, etc.)** The person who is required to be under the usage of this act is like:

- **Section 44A:** The person who is responsible for any furnishing of the document, didn't report to the authority or the company, then he is ought to pay the penalty or take the punishment. The document or data given to him must be returned to the authorities with the same content except the security modification, if he/she failed to do it, then they come under this act. This is imposed just as a punishment for the person in not protecting or preparing the data. This section also comes under only when the reality is proved and not just by the allegation by the company. When the proofs are submitted, then the penalty or punishment, one of these both is imposed. The person who (**The penalty would be not more than 1.5 lakhs or given a punishment of 3 years for each failure).**

- **Section 44B:** The files to be furnished or prepared and the documents to be returned, must be done within the specific time mentioned by the company or authorities. The files or work allotted must be submitted in the time given by the company as per the regulations. Or else there is a chance of compensation that

to be done by the person. **(Penalty of 5 thousand rupees for everyday that failure happens).**

- **Section 44C:** If the person is allotted to maintain the records, files, documents or data base, is he fails to do the same thing and in any case was the reason for the leakage or loss of the information, then he is subjected to a penalty. **(Penalty of 10 thousand rupees for everyday that the failure happens).**

- **Section 45: (Residuary Penalty-failure in following the rules and regulations)**
  Under this section, if anyone does not follow the rules and regulation made under the act in the company/organization must be subjected to a penalty. That is, if any employee of the company exceeds the rules and regulations of the company then he is subjected to a penalty. **(Penalty not exceeding 25 thousand rupees).**

- **Section 61: (Civil court don't have jurisdiction)**
  In the authority of the cybercrimes, no civil court is involved or have the power to reserve or stop the actions of the Appellate court under IT Act. This is the major difference from the IPC and IT Acts. No other court or power has the authority to oppose or interfere in the actions taken by under this act.

- **Section 62: (Appeal to the high court)**
  However, any person who is not satisfied with the decision of the Appellate tribunal (court under It Act), they can appeal to the high court if they want to challenge the decision. There, if the high court feels that the appellant is on the right side, it considers his appeal and goes through it. After the listening, the court gives its decision. The appealing time must now exceed 60 days after the judgement from the Appellant court.

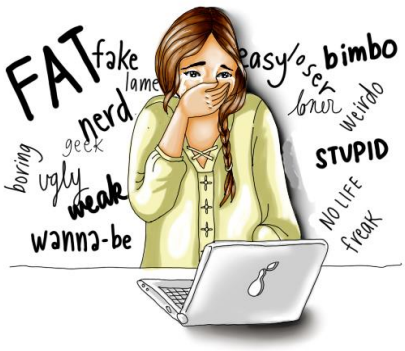
fig: High court of Andhra Pradesh.

- **Section 65: (Tampering with computer source documents)**
  The person who ever intentionally destroys, modifies or alters or helps the person intentionally who want to modify, destroy the source code of the computer, computer program or computer system. There is a compensation for this kind of crimes. Tampering indicates change or modification of data with respect to the original copy of the file to mislead the user who use the information intentionally. This **(Punishment of 3 years and penalty of 2 lakh rupees, either one of these two or with both of them).**

- **Section 66: (Computer related offenses)**
  Any person with an intentional mind to do the crimes related to the section 43, he shall be punishable with imprisonment and penalty.

- **Section 66A: (Punishment for sending offensive messages through communication services that can be proved, etc.) (Cyber bullying)**
  Any person who is sending information by means of a computer or communication service which is:
  - Offensive to the receiver.
  - A false information that the sender too knows it, but to cause mental disturbance to the receiver, annoyance, danger, insult, criminal thought, hatred and bad results by using the computer or communication service.
  - An electronic mail or message that may cause annoyance or mislead the receiver and make him in fake belief in such messages.

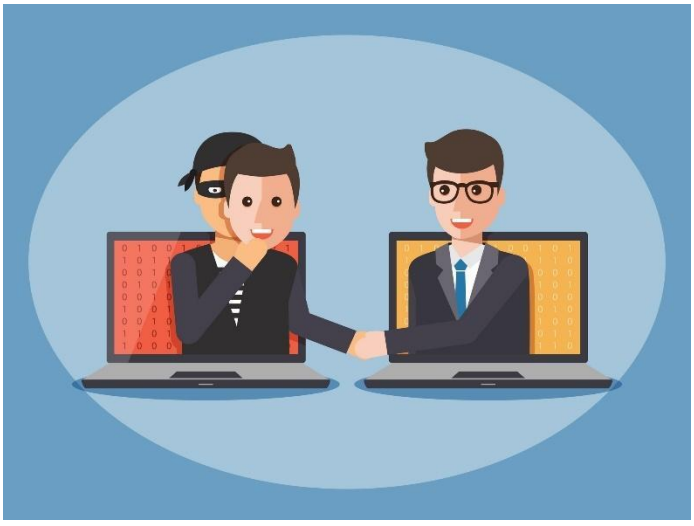
  These above mentioned are punishable with imprisonment as well as penalty. **(Punishment with 3 years of jail and 2 lakh rupees fine).**



- **Section 66B: (Punishment for dishonestly receiving stolen computer resource or communication device)**
  Any person who receives the stolen computer devices or its parts with knowing that they are stolen ones, and if those are retained from them by the authorities,

then the person is also highly punishable with imprisonment and also penalty. **(3 years of imprisonment or 1 lakh rupees fine sometimes with both the penalty and the imprisonment).**

- **Section 66C: (Punishment for identity theft)**
  Any person who ever dishonestly use the electronic signature, password or other authentication meters without the knowing of the original person is subjected to a penalty and imprisonment. **(3 years imprisonment and 1 lakh rupees penalty).**



- **Section 66D: (Punishment for cheating by personation with computer resource)**
  Any person using communication device or computer systems cheat any person, then it is termed as a crime under this section. He/ She is subjected to

punishment and penalty. **(Penalty not exceeding 1 lakh rupees and punishment of 3 years imprisonment either of these two, or with both).**

- **Section 66E: (Punishment for violation of privacy)**
  Any person who is intentionally capturing and publishing images of private area of any other person without the permission of the person and sending it other person/persons intentionally and to make others also view it though digital media, computer system or any other communication device. This is considered as a crime under this section and compensation should be made. **(Penalty of not exceeding 2 lakh rupees and punishment of 3 years imprisonment).**

- **Section 66F: (Punishment for Cyber terrorism)**
  Any person with intention to threaten or disturb the unity, sovereignty of India or to bring fear in the people of India-

- By denying access to person's own computer resource which the person is authorized of.
- Trying to penetrate a computer which is not authorised to him/her or trying to exceed the authorization by using illegal techniques.

- Trying to install or installing a bad software/malware which is harmful to the computer/computer resource.

which leads to damage the sovereignty, unity, strength of the people of the country.

- The person trying to penetrate into a system/ computer resource which if proved to leak the confidential information of any state or the country, it is termed as cyber terrorism.

This leads to a heavily punishable offense with imprisonment that may lead to life time imprisonment later.

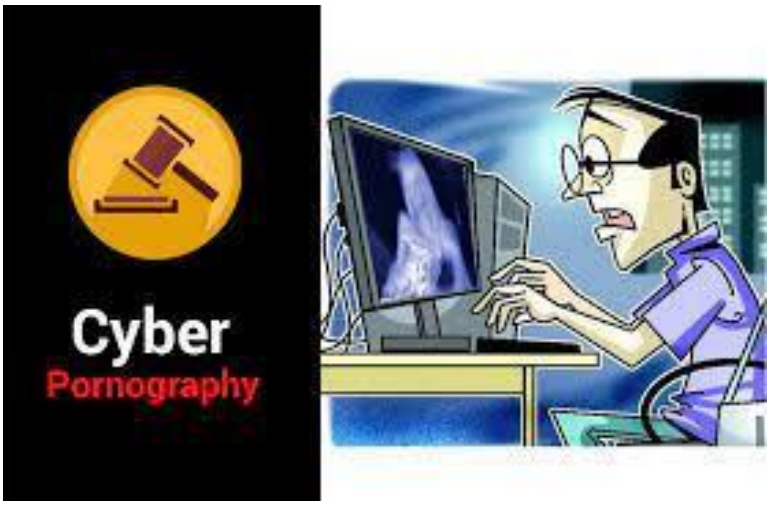
- **Section 67: (Punishment for publishing or transmitting obscene material in electronic form)**

Any person who is trying to publish or transmit or the reason for publishing or transmitting of a material which is related to nudity and it is intentional to affect the person who is going to see it, then the person who made this publishing is highly punishable for an imprisonment and penalty.

(Penalty which may extend to 5 lakh rupees and imprisonment which may extend to 3 years when it is the first time. If the same person or the company, does it for second time, then the imprisonment extends to 5 years and the penalty to be paid extends to 10 lakh rupees).

- **Section 67A: (Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form)**
  Anyone who is publishing or transmitting or trying to help the person who is publishing or transmitting or the reason for publishing or transmitting the sexually involved content in electronic form shall be punished and subjected to a penalty if it is the first time. **(imprisonment which may extend to 5 years and penalty which may extend to 10 lakh rupees).**

If the same person commits the mistake for second time, then the person will be punished severely with imprisonment and high penalty. **(Imprisonment which may extend to 7 years and penalty which may increase to 10 lakh rupees).**



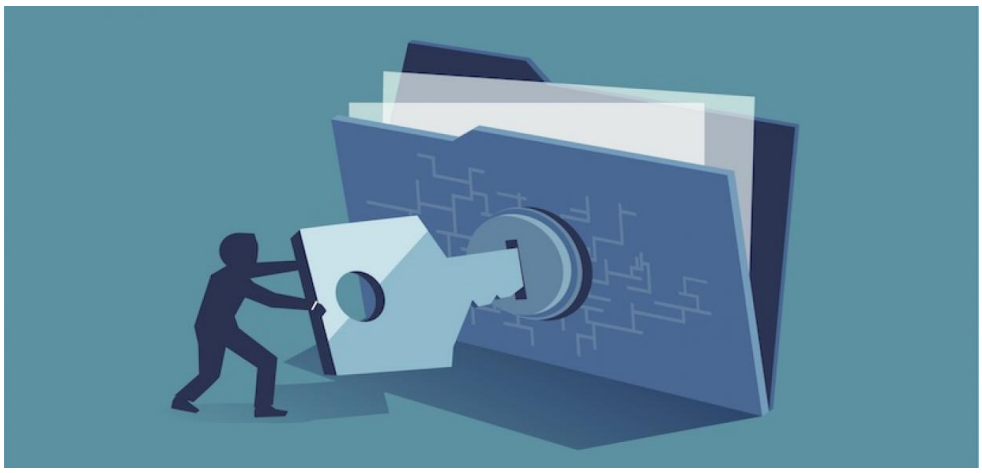
- **Section 67B: (Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form).** Anyone who publishes or transmits or cause for the transmission and publishing or helps in publishing –
    - Data which involves children in sexually explicit way through electronic form.
    - Data, images and collects, browses, downloads, advertises, promotes or markets the material in electronic form showing children in an obscene way.
    - And encouraging children for relationship online with one or more children for the moto of sexually explicit acts on computer system or through any electronic form.
    - Abusing children online also involves under this act.
    - Records the sexually explicit acts involving children in any electronic form or computer system.

  With involving any of these, the culprit who committed the crime shall be punished. **(If it is the first time, the person is punished with an imprisonment of 5 years and penalty of which may extend to 10 lakh rupees. If the same person has committed the mistake for second time, then the imprisonment is done for 7 years and fine which may extend to 10 lakh rupees).**

- **Section 67C: (Preservation and retention of information by intermediates)** The intermediary must keep or preserve the information secretly which is prescribed by the central government for a duration said by them. Until then, the intermediary is not allowed to leak or tell that information to anyone. If the information is leaked by the intermediary, then the person can be subjected to imprisonment and a penalty. **(imprisonment which may be extended to 3 years and penalty defined by the authority).**

- **Section 69: (Power to issue directions or interception or monitoring or decryption of any information through any computer resource).** The Central government or State government or officers who are officially authorized by the Central or state governments, if satisfied to do, in the view of

sovereignty, integrity or unity of India or security of the state or security of India for preventing any cognizable offense relating to the view and interest of the substances mentioned, reasons to record, write, by order, direct any agency of the state or central government to monitor or decrypt or know any information from any stored information of the computer resource.



The user who is the owner of that computer resource, when called by the agencies officially should give access to their computer, if found to be involved in any of the offenses and the agency is also supposed to keep the information personal to him to be safe and secured and do not leak it outside except the found malicious content. **(imprisonment of a term which may extend to 7 years and also penalised).**

- **Section 69A: (Power to issue blocking to public access of any information through computer resource)**
  The Central government or State government or officers who are officially authorized by the Central or state governments, if satisfied to do, in the view of

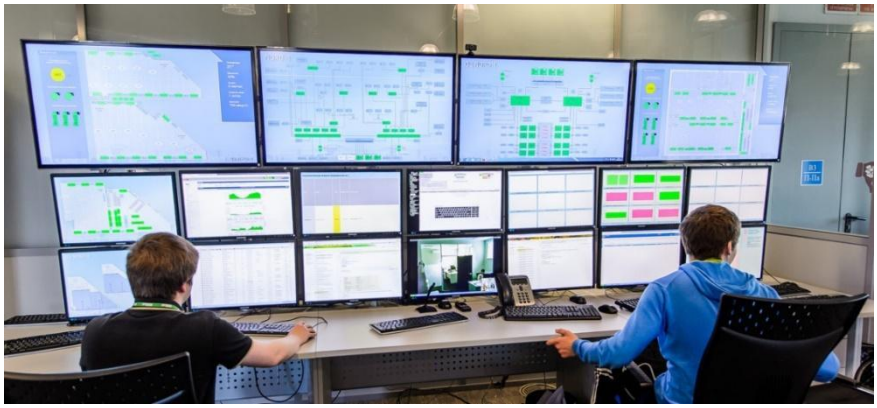
sovereignty, integrity or unity of India or security of the state or security of India for preventing any cognizable offense relating to the view and interest of the substances mentioned, reasons to record, write, by order, direct any agency of the state or central government to block any access to the public of a particular information that is offensive as mentioned above which is shared, stored, generated, transmitted or the reason for generating in any computer resource. This procedure secures that information from reaching public. The intermediary or the owner of the computer resource who fails to explain the well reason will be subjected to punishment and penalty. **(Imprisonment which may extend to 7 years and penalty fined by the law).**

- **Section 69B: (Power to authorise to monitor and collect data or information through any computer resource for cyber security)**
  The central government may issue a notification by official gazette, in order to enhance the cyber security and prevent malware content in the computer resources in the country, to prevent the intrusion of computer contaminant or malware into the computer systems/computer resource, authorises an agency to collect, record and monitor the data collected from the computer resource which is generated, stored, transmitted or received. The intermediary or the person who is owner of the computer/ computer resource when called by the agency, if not cooperated and found the reason for the crime is him/her, then he will be punishes and penalised. He/she even must provide access to the authorized agency from the government. The intermediary who does not follow the instructions of the agency will be subjected to punishment. **(Imprisonment which may extend to 3 years and a penalty will be decided).**

- **Section 70: (Protected system)**
  The government may give orders to announce any computer resource as protected which directly or may be indirectly affects the infrastructure for critical information. The government in the same announcement authorises a person or team to access the computer resource. Any person who secures or secures the access to such protected computer resources, will be subjected to imprisonment and penalty. **(Penalty is fined on him which is decided by the government and imprisonment which may extend to 10 years).**
  The central government also prescribes the cyber security measures and protection ways to such protected system.

- **Section 70A: (National Nodal Agency)**
  The central government may decide any organization belonging to government as National Nodal Agency to protect the infrastructure of critical information. This agency will have all the powers and are responsible for all the measures in

protection the critical and confidential information of the government from attacks and malwares.

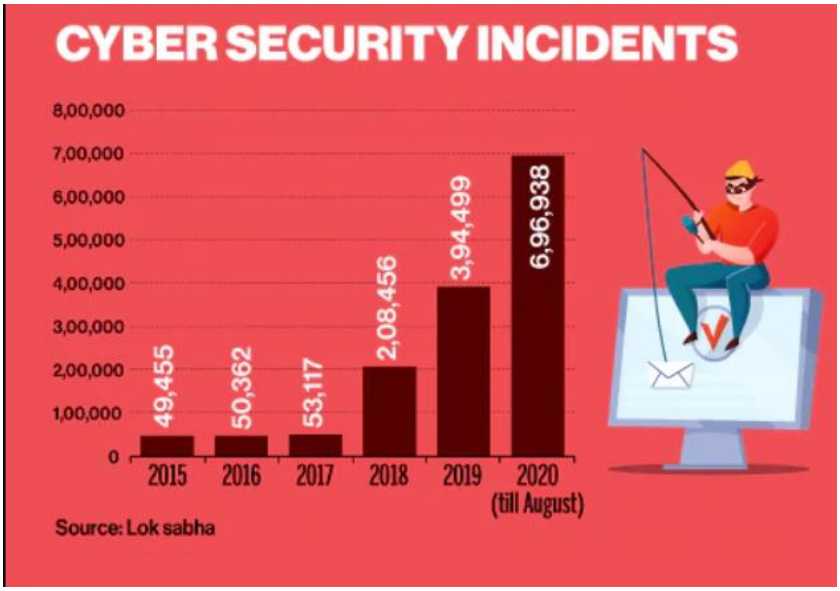


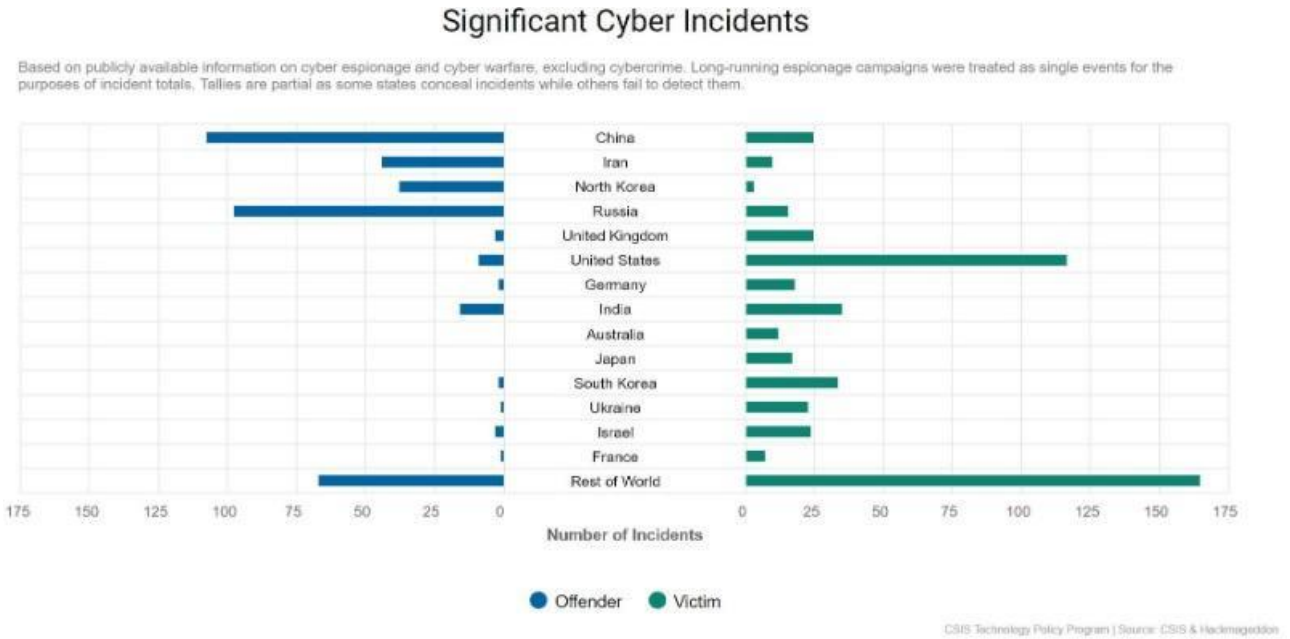
- **Section 70B: (Indian Emergency Response Team to serve as national agency for incident response)**
  The Central government has the whole right to announce in an official notification to appoint an agency belonged to government which could be called Indian Computer Emergency Response Team. The government itself provides a high-level officer as director general for the team and also provides employees and such other officers. The salary and other allowances will also be given by the government itself.

The Indian computer response team will be served as national agency for performing the functions of cyber security:

- Collection, analysis of cyber incidents.
- Publishes and alerts the cyber security incidents.
- Making emergency measures for the threats.

- Coordination between the activities.
- The manner of performing all these activities is prescribed by the organization before itself.
- For carrying out the security, the agency may give orders and guidelines to service providers, data centres, intermediaries, and others. If they do not cooperate with the agency of the central government, they are subjected to an imprisonment and penalty. **(Penalty of 1 lakh rupees and 1 year punishment)**
- No **Court** is subjected to take any actions on the agency for these actions under this section.





- **Section 71: (Penalty for misrepresentation)**
  Any person who ever misrepresents the or supresses any facts or orders given by the authorities or agency, or if they hide any detail from the certifying authority for obtaining license or certificate, they will be punished and penalised. **(Penalty which may extend to 1 lakh and imprisonment which may extend to 2 years).**

Most of the fake information is seemed as fact, Beware! Check the information before you believe.

- **Section 72: (Penalty for breach of confidentiality and privacy)**
  If any person is involved in the breaching of the confidentiality and privacy of the Computer/Computer resource which is to be used by another owner. If it is manipulated or attacked by any person who is not the owner or who has authorized access to the system, intentionally to create a fuss and also to leak the data from that computer resource or electronic form. If the data is leaked

intentionally with interest to know the data without authorized access creating a data breach which interrupts the privacy of the person who is the original user of that computer resource. **(Penalty of 1 lakh rupees or imprisonment which may extend to 2 years or with both).**

- **Section 72A: (Punishment for disclosure of information in breach of lawful contract)**
  Any person who provides services, intermediaries, contractors, even the people who provide service with an official agreement or contract, has secured or saved access to any material or document containing personal information about the other person who took services from them with an interest to cause damage to the person by keeping the personal information in public which causes loss to the person or if he try to sell the data or even manipulate the person with the data he have, then he is subjected toa punishment and also penalty.
  (imprisonment which may extend to 3 years or penalty which may extend to 5 lakh or with both).

- **Section 73: (Penalty for publishing electronic signature/certificate false in certain particulars)**
  Any person should not publish a certificate or electronic signature which belongs to them or others in the knowledge of knowing that the certificate is not issued by the concerned authority shown in that certificate, or the certificate is not accepted by the concerned person named in that certificate, or if the certificate once owned has been revoked/taken off otherwise suspended. If any person who does these above-mentioned activities. The person is subjected to penalty and imprisonment. **(Penalty which may extend to 1 lakh rupees or imprisonment which is for 2 year or with both)**

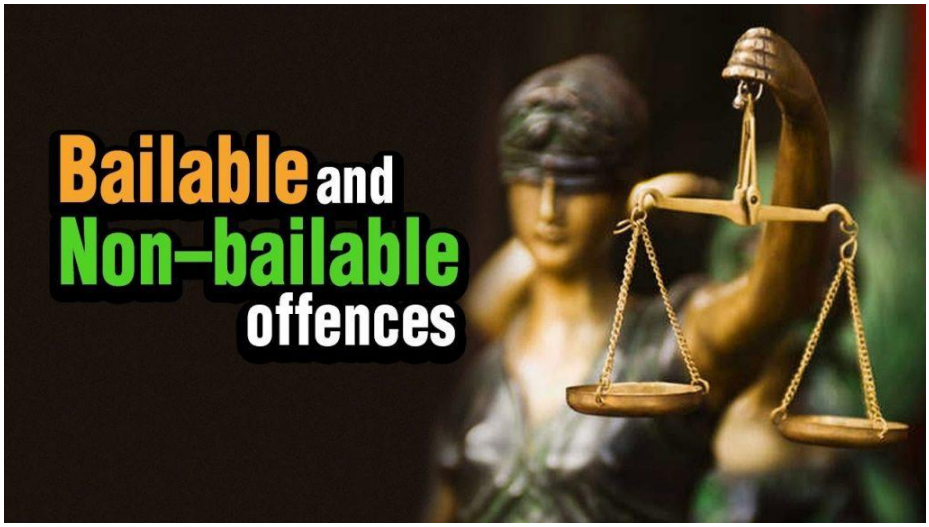
- **Section 74: (Publication for Fraudulent purpose)**
  Any person intentionally, knowingly made or publishes an electronic signature or certificate for wrongful purposes or fraudulent purposes shall be punished and penalised. **(Imprisonment of a term which may extend to 2 years or penalty which may extend to 1 lakh or with both)**

- **Section 75: (Act to apply for offence or contravention happened outside India)**
  Any person who has committed to an offense or contravention outside India is subjected to come under this law. This act will apply to the people outside India irrespective of nationality, until the system affected or computer resource targeted is located in India.

- **Section 77: (Compensation, penalty or confiscation not to interfere with other Punishment)**
  Compensation awarded, penalty imposed or confiscation made under this section will not prevent other compensation or imposition of any other fine or punishment under any other law.

fig: Compensation and confiscation.

- **Section 77B: (Offenses with three years' imprisonment to be bailable)** The offenses committed under any of the sections which is subjected to an imprisonment of more than 3 years is Non-bailable or Cognizable. The offenses which are with imprisonment less than 3 years or 3 years are bailable.



- **Section 78: (Power to investigate offenses)**

For all the sections in the law, the power to investigate is not with all police officers. The police officers who are not below the range of Inspector only supposed to investigate the courses.

Introduction to Cyber Security:

Elements of Information Security:

The Information security is continuous process. It is the process of preventing harmful and unauthorized access, also preventing modification, altering, analysing, inspecting, destroying the data or information from other persons or attackers. The information is not accessed by any other individuals or groups without the key to it which is only known by the user or owner. There are three principles of information security:

1. Confidentiality.
2. Integrity.
3. Availability.

1. **Confidentiality:** Confidentiality is making an information very private that no one can access that information. That information may be the main secret or base of that company, which should not be known by any other person except the authorized person. This principle ensures us that the private information will be private and will only be accessed or viewed by people who need that information to take company forward.

2. **Integrity:** Integrity principle gives us the trust that the data under the security is not changed. The data, documents, files, storage under the security can't be modified, altered or rewritten. This ensures that the data can be trusted and not modified without the authorization.
3. **Availability:** Availability is protecting the data and making it available to its users when it is in need to them. It is ensuring that the data is available fully at

any point of time when it's needed by the company to make decisions. The authorized person only gets the information availability.

fig: Information security CIA Triad

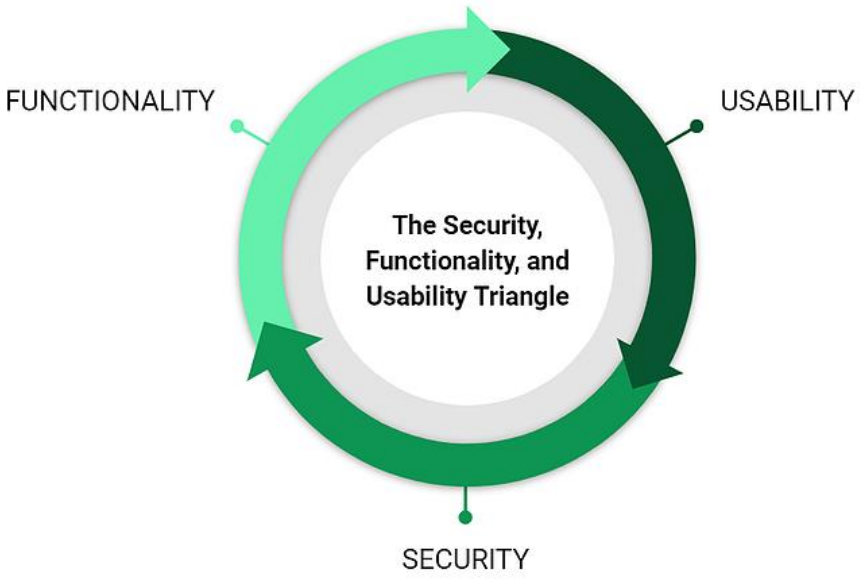
Important Characteristics of Information:

There are three important characteristics of information, they are relative to each other

1. Security.
2. Functionality.
3. Usability.

The Security, Functionality and Usability are relative to each other. They are interlinked with each other. When one goes up the remaining two goes down. Suppose, the functionality goes up, then Functionality and usability comes down This perfect balance should be arrived by any company for balanced information system.

- **Security** --- The security of a system/ computer resource f a company**.**
- **Functionality** --- The performance of the system or the server.
- **Usability** --- The usage of the system is termed as usability.

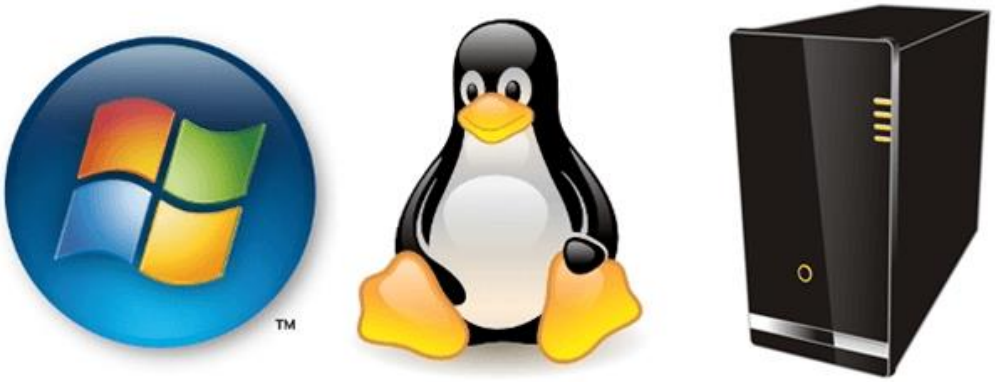


- ☐ If the '**Usability'** increases by the users or the customers, then the security and functionality decreases, due to the large amount of usage.
- ☐ If the '**Security'** increases, it does not give more space for the functionality and usability.
- ☐ If the '**Functionality'** increases, the security and usability decreases.

Non-Repudiation: The assurance that a person signed a data or generated an electronic signature in a deal, cannot later deny that the person didn't want the deal, until the proof is shown.

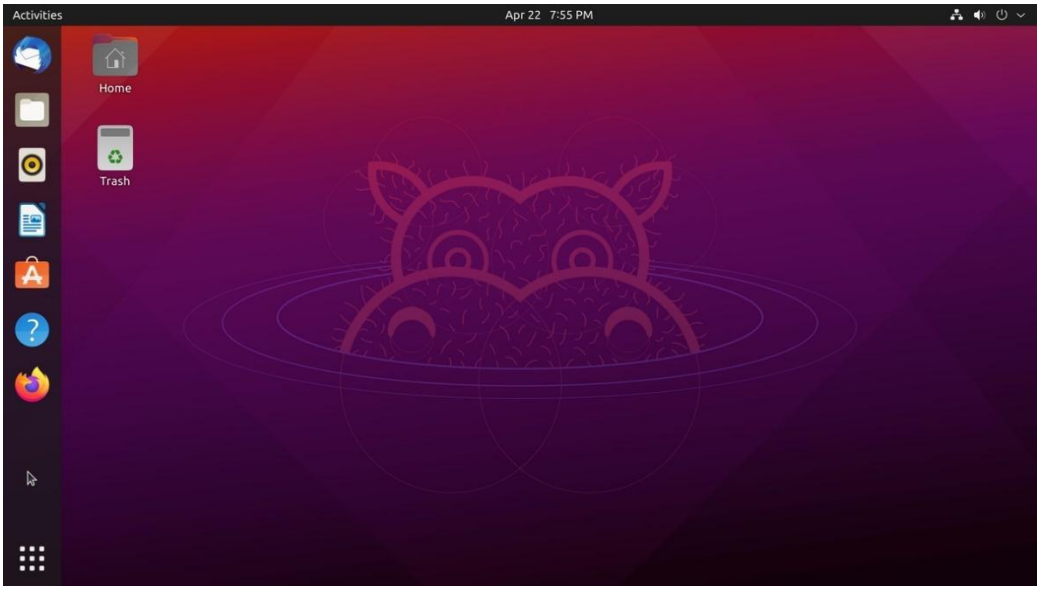
Generally, there is an analysis that the following systems have that specific characteristic more.

- **OS (Operating system):**
  It has more **Usability** characteristic.



- **Linux:**

It has more **Security** characteristic.



- **IOS:**
  It has more **Functionality** characteristic.

NOTE:

- If you feel any time that, you want to know the time taken to crack your password. Open Google and type<**How strong are my password**> you can check the strength of the password.
- To check whether your email is Pwned, type in google <**Have I been Pwned?**> you will know either your email is Pwned or not.

Information War-fares:

Information war-fare is modifying the information which is saved by a person without the authorization and without knowing it him. And then making him believe and keep trust on the same information modified and act according to the modifies information and indirectly guidelines set by the person who altered it. This leads to a stage that the original guidelines the user want to follow will not be followed and his company may go into deep threats.

There are 2 types of war-fares in information security. They are:

1. Offensive war-fare.
2. Defensive war-fare.

1. **Offensive war-fares:** Attack from one country to another country, there won't be any punishment for this, if it is on minor companies. It comes under Offensive war-fare. (with tools or in any other form through electronic way).

2. **Defensive warfare:** Defend or protect one's own country from attackers from other countries is called defensive warfare.

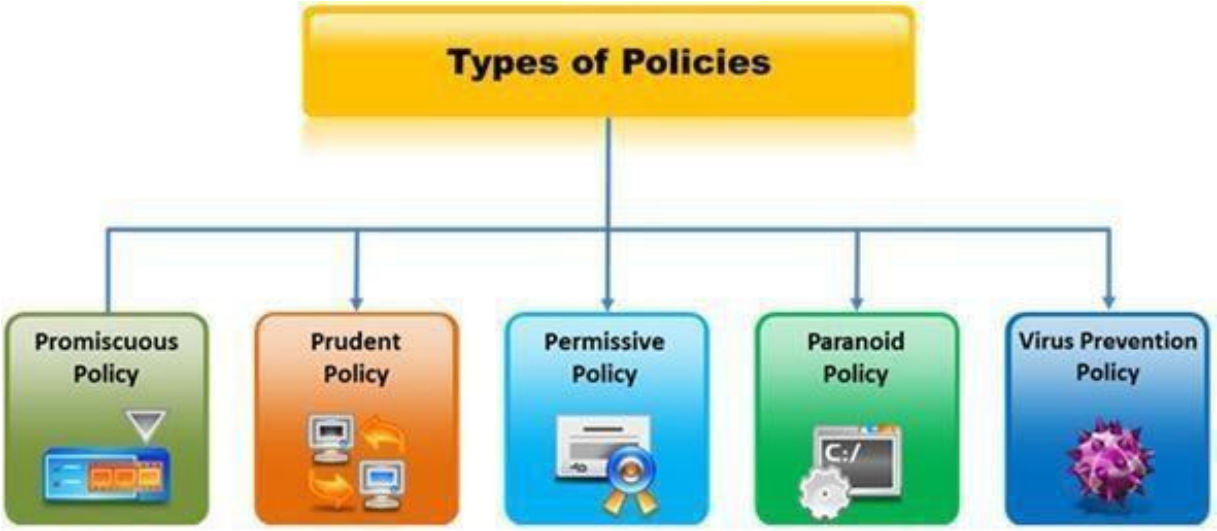
Information Security Policies:

Information Security Policies are the policies which every company must have which help them protect themselves from cybercrimes. Without the security policies no company can with stand in the market and protect them. The security policies are the

main pillar of any company, if they want to stand in the market, they must have security policies and protective measures.

There are many types of security policies:

1. Promiscuous policy.
2. Permissive policy.
3. Prudent policy.
4. Paranoid policy.
5. Virus Prevention policy.



1. **Promiscuous policy:** The policy which does not impose any conditions on the usage of the system/website. That means, in a company following the promiscuous policy give right to the employees to use the internet anywhere, the employee doesn't have any restriction on any website or applications and can access a PC or network from a foreign location. This may be useful to the companies where the employees work in travelling from one place to other like the loan recovery employees. Or, to the company which have branches where employees might want the access to the structure networks.
   Several malwares, viruses may be present in the public networks or free internets. The company owners or directors must be very careful while selecting this policy.

2. **Permissive policy:** Under this policy, the policy blocks the highly dangerous websites from opening in the system. It allows heavy traffic to the system, but do not allow the dangerous attacks and dangerous websites are blocked from

conducting action on our system. This helps in protecting the system from known dangerous services or attacks or behaviour. It can't stop the newly created dangerous attacks. It can only stop the attacks that the system is updated and ready. It is not possible for developers or owners of the company to keep in mind with the new attacks, they only develop the security in the policy for the attacks until the date of updating.

3. **Prudent policy:** In this policy, it blocks all the services in the internet and only allow the needed one for completing the job of the employee. It will not allow all types of services from the web, only allows a few one which are controlled by the owner of the company. This helps in preventing all types of malwares, trojans and other content to enter into the computer or system. It notes down all the logs and can't be changed or cleared.

4. **Paranoid policy:** This policy blocks everything, there is strict rule on the usages of the company computers or systems, whether it's system usage or network usage. There is no net association or strict rules on the internet usage. Because of these severe restrictions, there is way to control all the malicious activities done on the system which may affect the whole process of the usage.

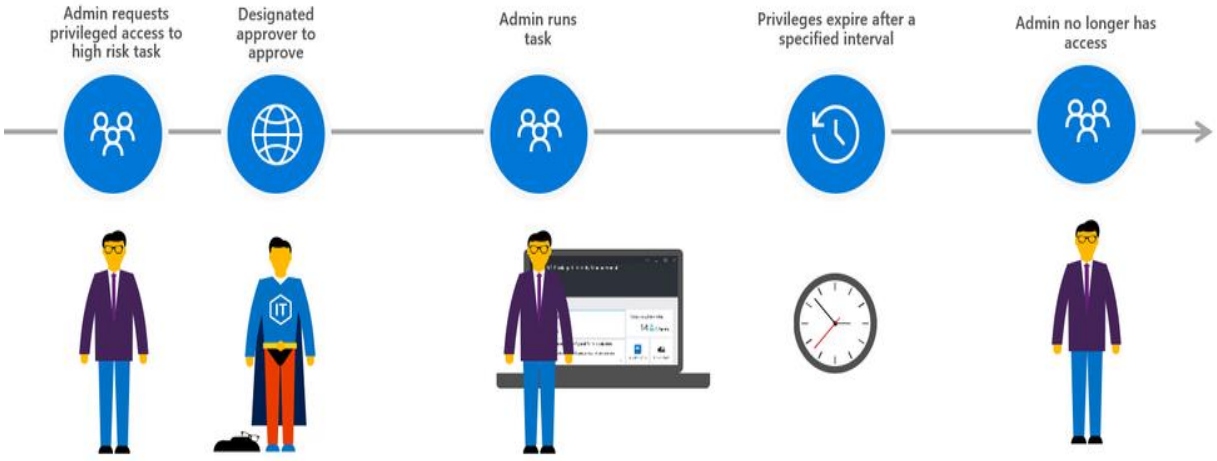
5. **Virus Protection policy:** This policy ensures that every system/computer which is under the policy must have an Anti-virus software installed in it on the network. All the Anti-virus must be running at all time and should have the log registering technology. This is used to identify and defend from the virus and sometimes deactivate the virus which stacked the system or the network.

Examples for security policies:

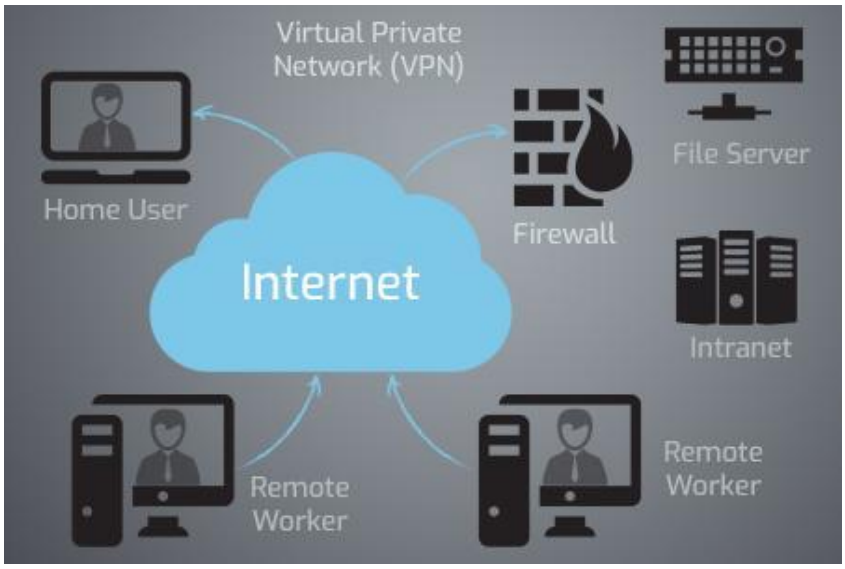
There are many security policies, some of them are:

1. Access Management policy.
2. Remote Access policy.
3. Firewall Management policy.
4. Network Connection policy.

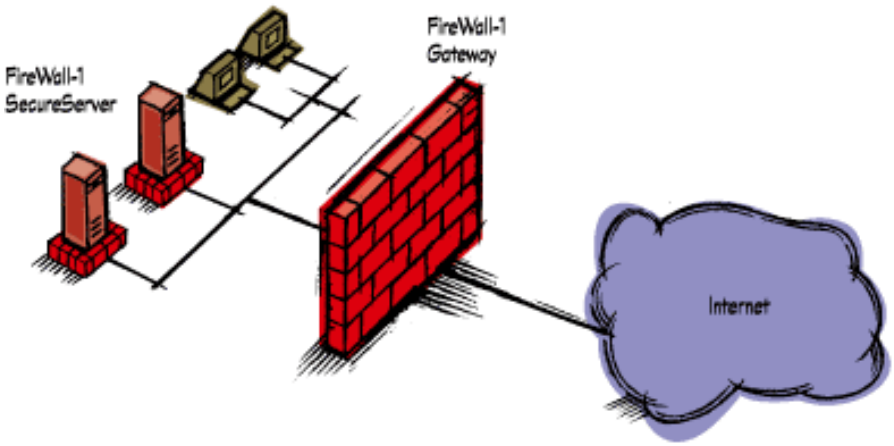
1. **Access Management policy:** It is a procedure of giving access to the information to the employee working in the network or the user with a correct cause of reason for taking the access. Even the multi-actor authentication is also applied on the person who wants to use the information for completion of their task/job. Their logs are and usage are also traced.



2. **Remote Access policy:** It is collection of set of rules which contain the rule who have the access to the system or computer. This policy is critical in big companies or organizations where the employees work from home. It defines the remote access permissions to every network or system working under the policy and creates a portfolio for it. This policy is used to safeguard the network from viruses, malwares, threats, and malicious injections to the network by observing the user behaviour, their intentions and profile of every connection made to the network.



3. **Firewall Management policy:** The Firewall policy defines how an organization need to protect its system and network from heavy website traffic and it explains the management of the inner and outside traffic of a network of a company. The firewall of the company should have the ability to differ between the company's system and other strange system which is a new one. It even should prevent the malicious content to enter the company's network. It should manage all the protocols or orders from the management based on the company.



4. **Network Connection policy:** This policy is used with all the computers and networks connected to the company network, without the specification of owners. In this policy, there is a special application and benefit that if any computer, PC or system connects to the company network, that system automatically accepts the policies of the network connection security. The user agrees to use the network only for legal applications and uses, can't use any other websites or applications other than these.

Physical Security:

Physical security is the protection of electronics, documents, data, hard disks, CD drives, files, other hardware, software from physical attacks like damaging intentionally and fire accidents, etc. This causes severe damage to the company, which in return give losses to the company financially.

This also includes and ensures the protection from fire accidents, floods, thunder storms and other natural calamities or disasters. Physical terrorism like bomb blasts include in the physical damage. So, to protect from these, firstly we need to make insurances on all the property we hold and we need to have security prioritization and keep the more valuable assets safely. This his main option of defence of the company. The first part of the security.

The threats are also divided into two types:

1. Environmental threats.
2. Manmade threats.

The measures that ensure the physical security are:

1. Security guards.
2. CCTV, Cameras.
3. Alarms.
4. Biometric system.
5. Fire safety.

Incident Management:

There are many steps involved in incident management:

1. Incident Identification.
2. Logging.
3. Categorization.
4. Prioritization.
5. Response.
6. Diagnosis.
7. Escalation.
8. Resolution and Recovery.
9. Closure.

- Find the detailed information of the incident and identify the reasons for the incident with clarity and error free and send to the authorities of the company like owner or manager. **(Incident Identification)**
- Note down all the damage caused and save the information to use it in further management. There should be proper information about the information and the reasons for it. **(Logging)**

- The collected information must be categorized into different forms and give a name to it. Like the damage caused in different departments and parts of the system and network. Like divide it into hardware, software, infrastructure, database, etc. **(Categorization)**
- Prioritize the information based on the damage it caused and note it in priority. The information is then separated into different forms based on the importance of the damage it caused and loss financially like low, medium, high priority. **(Prioritization)**
- Then respond to each of them based on the importance decided as before. **(Respond)**
- Know the steps to rectify the problems by diagnosing the damage information and have the knowledge of it and write down the ways. **(Diagnosis)**
- Now, escalate the differentiated steps according to the procedures and categorize into level 1, level 2, and level 3. **(Escalation)**
- Now, with all the required information and solutions, resolve all the problems due to the incident and damage. Recover all the data and try to back up to the new databases. **(Resolution & Recovery)**
- With all the problems solved and the damage capacity, recovered databases and other information, prepare a report and submit to the higher authorities with clarified explanation from the start to the end. **(Closure)**

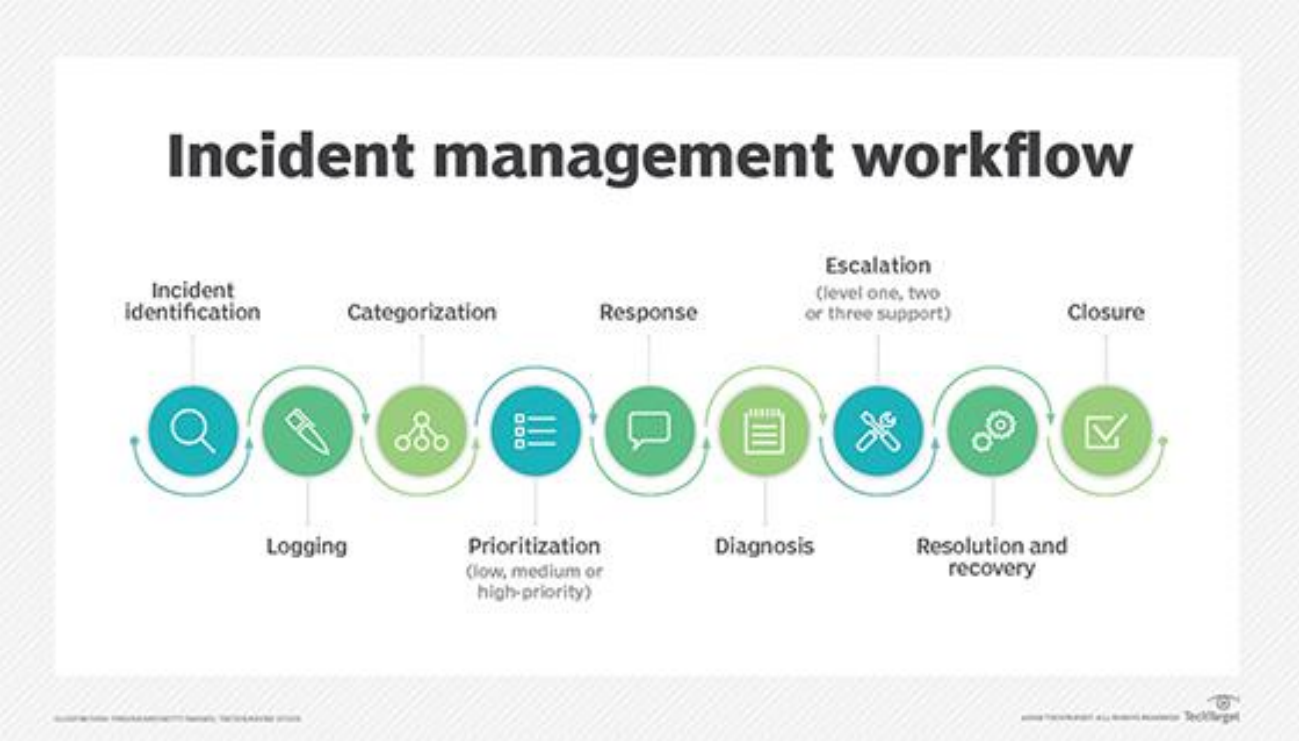
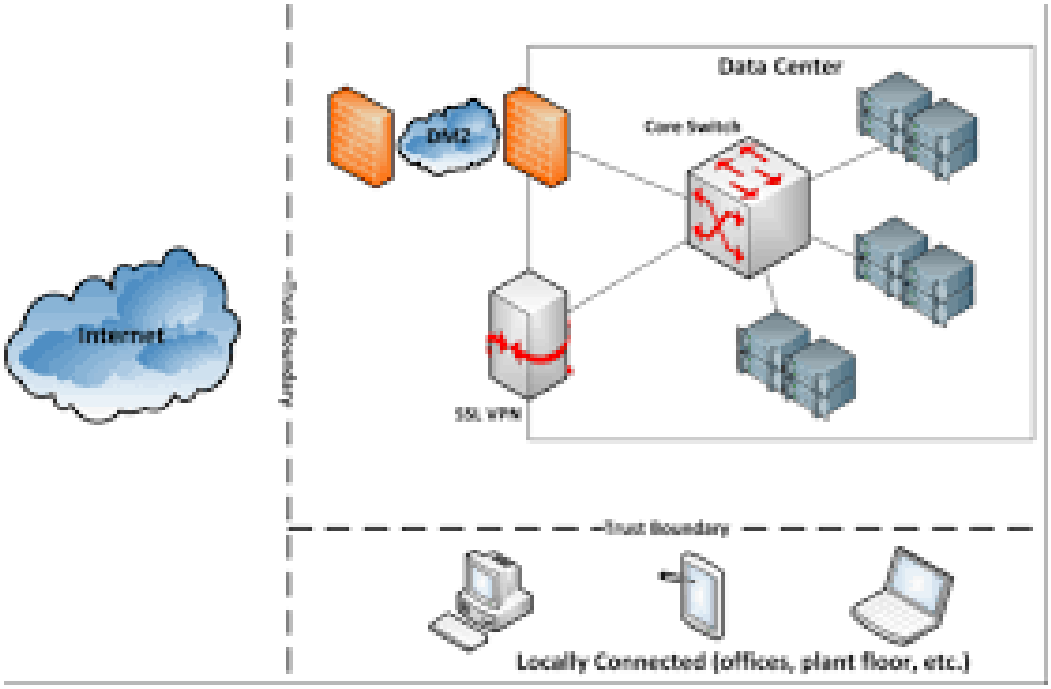


fig: The Incident Management workflow.

Network Security Zoning: In this, there is separate zoning for all types of departments and sectors. The person who is handling all these will have the access to the network and any person, if need the access, he needs permission or authentication of that person to connect or use that network files.

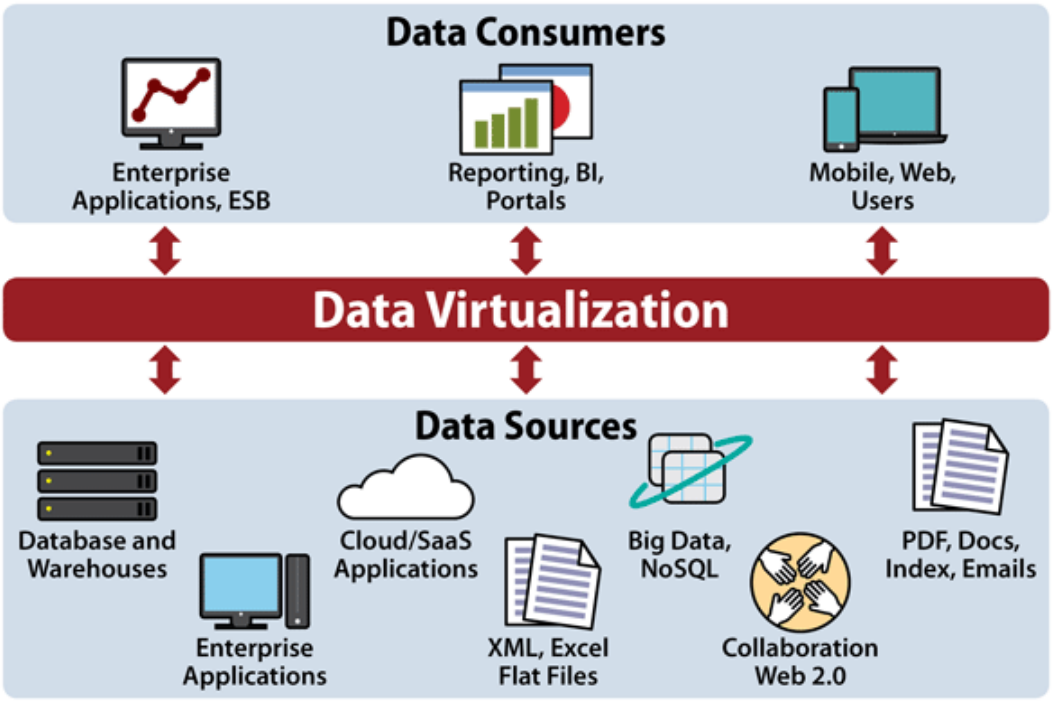


Virtualization: Virtualization is operating or using more than 1 OS on the same PC and can run them in parallel. The virtualization is very useful to know various behaviours of operating systems in the same PC. We use the Virtual box to access the virtualization, we can install many operating systems (OS) in a virtual box, can also install the android in the virtual box still being in a PC/computer system.

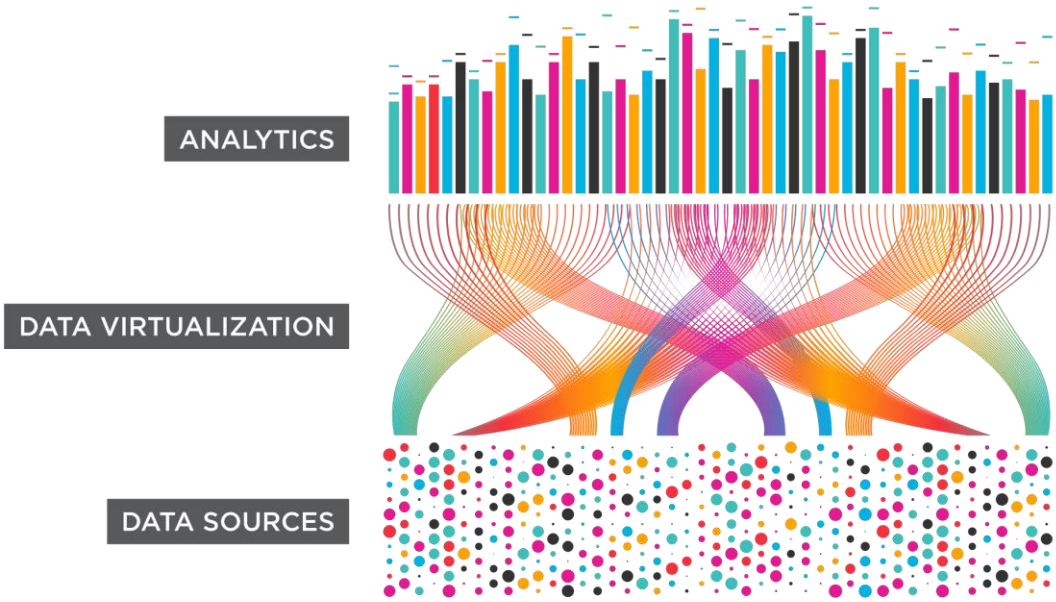
This virtualization is very useful to install all kinds of software in a single PC with respective of the software's best working OS. This enables the efficiency of the computer and its work. But the virtual box must be installed in a PC which is of little bit high RAM, to support the parallel running OS and software. This process is also very useful in hacking and ethical hacking as well. Most of the hackers use the virtual box to hide their identity and also use the hacking tools without getting the main PC effected and damaged. This is called virtualization. These are the types in virtualization:

1. Data Virtualization.
2. OS Virtualization.
3. Network Virtualization.
4. Server Virtualization.

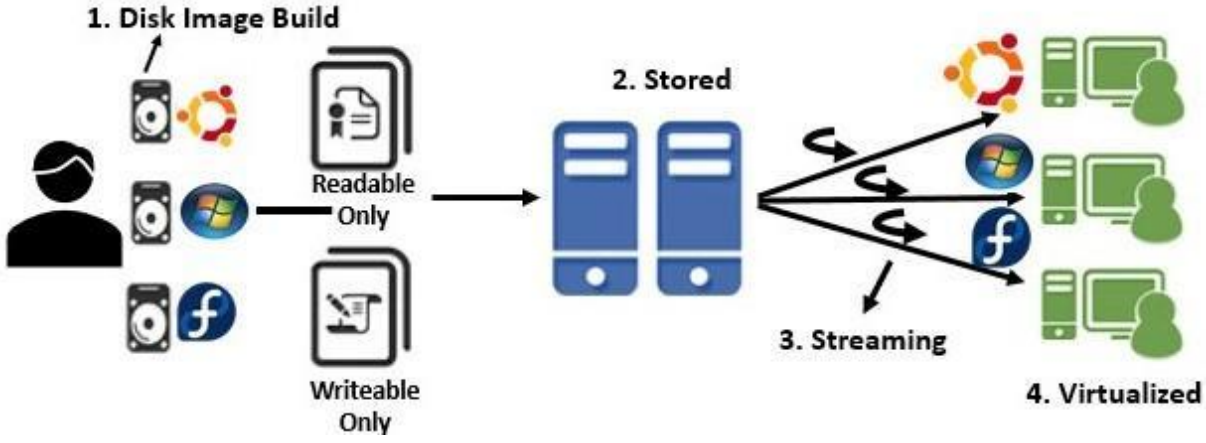
1. **Data Virtualization:** It is a management technique of data that enables an application to retrieve and manipulate data without requiring technical details of the system or file like address, location, key, etc. and provides the data view which enables to access the data. The data is directly accessed by the consumers from data sources through this technique.



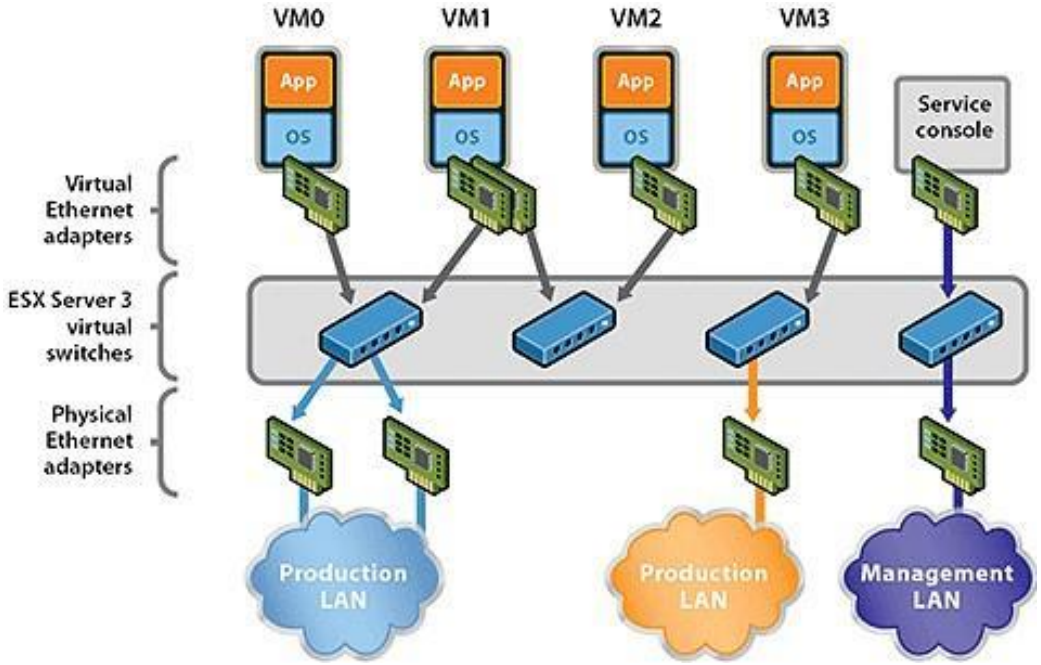
The data sources and their usage with some other information, it is shown as some analytics which is called Data virtualization.

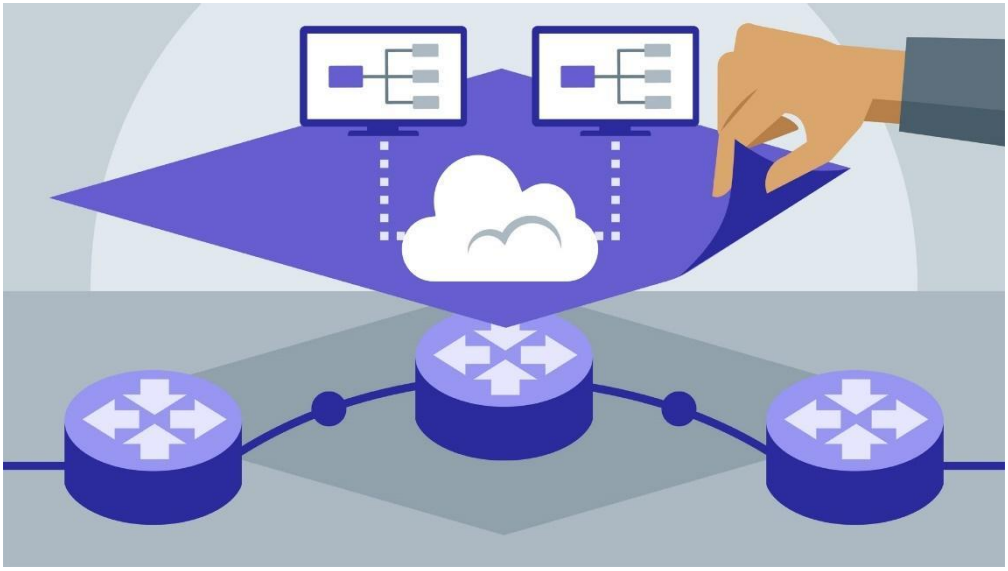


2. **OS Virtualization:** It is using or utilizing an OS in a system or PC in which already an OS is present. That is, the newly installed operating system interacts with the operating system which is already present in the system with a single layer of hardware. Here the PC in which the virtual box is installed to handle the new OS, it must be at least a system of high RAM than a usual one to use both the operating systems pin parallel.



3. **Network Virtualization:** Network virtualization is the process of combining software and hardware together into a network which is having all the data and resources and its functions which is controlled by a software, in a virtual network. It involves many platforms virtualization which is combined with resource virtualization.





4. **Server virtualization:**
   To know about server virtualization, we need to know about the hyper-visor. The hyper-visor is also known as a virtual machine monitor (VMM) that creates and runs the VMs and the systems. This allows computer or PC to allow multiple guests or use this as host to access multiple guests. The server virtualization is separating or dividing a server or data base into several system which can host many other systems as hosts. This is called server virtualization.

Traditional Architecture Virtual Architecture

The same server is used as different servers for the systems and PCs which are on the same network.

Skills required for an Ethical Hacker:

There are some technical skills required for ethical hackers:

1. Technical skills
2. Non-Technical skills.

1 **Technical skills:** The technical skills required for an ethical hacker are like:

- Coding to some extent, need not to know full coding.
- Networking with the software and hardware of the systems and their inner knowledge.
- Techniques for finding the vulnerabilities, idea is major task here, the ethical hacker must have the idea about all types of data in the computer which is to be stored.
- Reporting the found data is the main concept which differs hacker from ethical hacker. He needs to report the work he is engaged with in. And also, he must report the outputs along with the process he followed.
- The ethical hacker must have the knowledge of usage of the hacking tools along with the methods of hacking.

2 **Non-Technical skills:** The non-technical skills are not much to be learnt.

- Communication skills are also essential skills to be learnt by an ethical hacker.
- Problem solving skills are also very essential to be an ethical hacker.

Data Breaches:

Let us know about some of the latest data breaches in the world.

There are many data breaches down in the year 2020 and even in the year 2021, The latest data breaches are very crucial and caused a huge loss as per the information and also revenue. The Data Breaches are like an unknown or anonymous hacker sending a malware into the organization set of data and using it to infect the whole information of the organization. Most data breaches are caused due to small vulnerabilities or negligence of the employees. Without the prior permission of the cyber security department of the company, most employees use their credentials even for other systems or websites in order to keep same credentials everywhere, so there comes the problem of leakage od credentials, even if the company security is very protective, with this easy way of getting credentials most data breaches are happening. These small vulnerabilities effect the whole system and even the data bases which is the reason for data breaches. Let us see some of the Data breaches:

1. **Marriott International: (Fact: Official Accommodation partner for Mumbai Indians IPL team)**

It is an international group of hotels which is actually a very big brand in hotel business. It provides very Elite services and have a lot of star hotels like five-star, four-star hotels. In the Organization data, Data breach took place on march 31st,2020.

"Unexpected amount of customer data is being accessed by unknown persons"

- Statement given by Marriott International.

The Breach happened through the login credentials of two employees of Marriott which led to the access of huge amount of customer data leaded to '5.2 Million customers' data. This is a major security breach in the history that would be in top 20 data breaches. The lesson learnt from this is that, to secure data of customers, you have to control how the employees access data rigorously. This could be avoided by using multi-factor authentication to the employees who access the sensitive data. While the expected breach of data may leak the following:

- Email address.
- Mail addresses.
- Phone numbers.
- Gender
- Birth dates.
- Company names the customers work for.
- Accommodation preferences.
- Language.
- Linked Airline services.

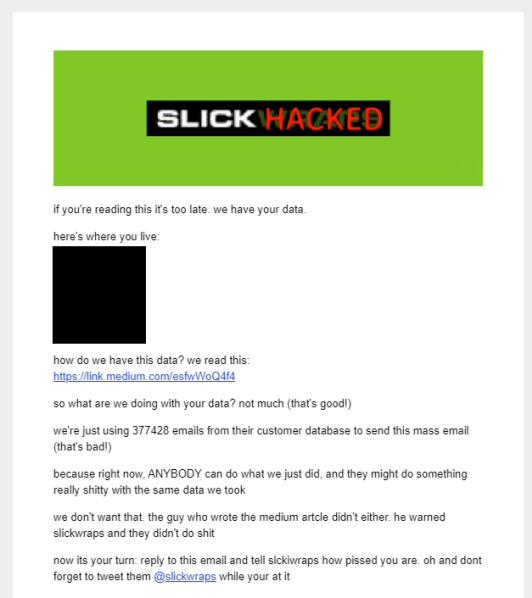
However, the company said about it in a later press note that the breach didn't leak the passwords of the account of the customers, Payment information, pin numbers. Marriott stated that by continuous scanning of data and as mentioned above with multi-factor authentication for login, it could prevent the company system/website from future data breaches.

2. **Slick Wraps:**
   Slick Wraps is a company which provides the customers the customized skins for their electronics. A White hat hacker warned them about this vulnerability and posted an input called “comically bad”.

But the company ignored it and didn’t care about it. He posted about this “abysmal cybersecurity”. Another hacker who read about this vulnerability, hacked the site and stole the personal data of customers like mails, phone numbers, gender, age, country, billing and shipping addresses and much other information which is definitely a major resource for the hacker. This breach took place in February,2020. Over 3,70,000 customers of slick wraps were under the impact.

The company name displayed in the website is also changed to “Slick Hacked”. A mail is also sent to all the customers stating that their account is hacked.

This is what happens when you don’t care about white hat hacker’s warnings.



3. **SolarWinds:**

   There is a data breach on the famous electronic problem resolving company which is a network monitoring software itself helps in protecting the data of companies and enables to detect and correct the vulnerabilities and find the risks to help us know them and protect from them. It increases the protection levels of the system/computer. This data breach affected the solar winds very badly which in return affected many companies and their businesses which happened in March,2020. There are approximately 18,000 businesses which are solar winds customers or users affected. The hackers who are the reason for this data breach are believed to from the Russia, nation state hackers. They manipulated a DLL link which is to be sent as an update to the “solar winds” users. This file is not officially sent by the authorities but seemed to the users as official update. So, most of them installed this and were affected with the malicious link. However, solar winds found the malicious activity which behaviour is weird and sending the confidential information to some other source which is outside the network.

By the time it is found, it made the damage successfully for a vast amount of users approximately 18,000 users and their businesses with their secrets and management. There are 6 U.S government organizations also involved in the breach. But this finding out the data breach was not discovered until December.

4. **Live Journal:**

The data breach occurred in the live journal which exposed the data of approximately 15 million people, which is almost 40% of the population of Canada. The Live Journal is a Canadian based company. The company's data breach happened due to the less staff in the cyber security sector. The chief cyber security head is responsible for this data interruption as there is negligence shown due to the lack of staff and resources. The data of the users like health card numbers, country Id numbers are accessed by attackers which enabled the hackers to get the whole data of the customers. Even the birthdates, login IDs, passwords and names were being got by the hackers.

The company suffered with this data breach in the year 2014 which is the result of 15 million people at the start as mentioned and later discovered to have breached 26 million people data.

Then later in 2018, most of the subscribers of the journal found that their password is changed to their old password which they changed it some years back. This happened because still some people are using the data of them and breaching the website. The people found this as they got the mails of password change to their mail address. Then later the HIBP (Have I been pwned) website announced that it received a file which containing the user information like usernames, email addresses, passwords that are weak and some basic information of 2\the 26 million people which it later published he names of them on the website to help them know and change the passwords and protect the data.

5. **Easy Jet:**

Easy Jet is a low-cost airline which is a very famous airlines company. The Data Breach is happened with the company's data. In this breach approximately 9 million customers data is being breached and accessed. This is not said by the company for more than 3 months to the customers. This leaded to breakage of trust of customers. The breach concluded that the data being accessed is the travel history of the customers, names, ages, birthdates, country and passport IDs of 9 million customers and the employee's details of the company. The credit card details of 2200 people including the credit and debit card numbers along with the CVV which should be secretly maintained by the customer. This may lead to the theft of the money from the customers.

The data breach happened between October 17,2019 and March 4,2020. This data breach as mentioned above is comprised of email addresses, the passenger's personal details like gender, nationality, age, date of birth, names. The confidential details like bank details and card information are also leaked in

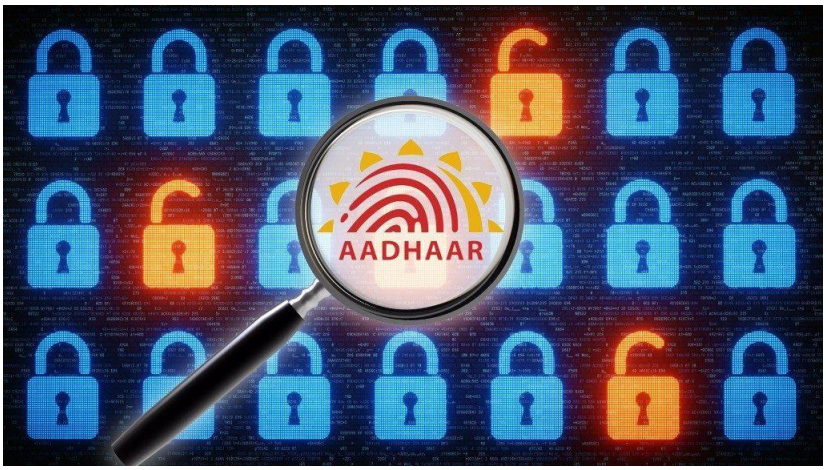
some cases. This breach made easy jet to secure their website with highly secured protective defence system as the breach effected the customers of easy jet and its sales. Easy jet also gave a press note about the breach and the security measures took because of it to prevent future attacks.

6. **Aadhaar:**

The Aadhaar data breach happened in March,2018. Aadhaar is the identity of the Indian citizen and it is the major one to get any of the services. It is the card given to say that the person is an Indian. In 2018, it came into the media that the Aadhaar data was being handled illegally and sold to private companies to gain profit. The data breach is such massive that 1.1 Billion Indian citizens data was leaked. This happened because of the data leak on a computer which is handled by a state government. This data hugeness is like the personal details of the citizens, information of them which is in the Aadhaar card, their specific 12-digit code and even the bank details of the people who linked their bank account with Aadhar.

AADHAAR

The Other information like, thumb prints. Retina structures and information and even the photographs of each and every citizen with their original address and other valid information is being known to the people who breached it. With this information, they can even trace the position of any person in the country, his location, as the sim card is being linked with Aadhaar. The sim card to PAN card, everything in India is linked with Aadhar. Later the breach is being detected and specific security measures are taken with all the organizations in the country.



7. **CAM 4:**

CAM 4 is officially an adult video streaming platform which even have premiums. The website data breach happened in March,2020. This breach exposed over 10 Billion records; this is the biggest data breach till date in data size. The breach is caused from the search server of the website which had little vulnerabilities and the hackers used this to breach the entire records as the search has access to the database which we know already.

The data is very vast that it includes details like email addresses, IDs, usernames, real names, phone numbers, debit/credit card details of the people who are the premium holders of the websites. The information also contains the details like the people's decisions in choosing, interest on a gender, interest on a

particular aged people, and sex orientation interested by that person. The hackers also known the information like payment logs, password encryptions, IP addresses, time spent on that adult site. And the major loss for the website is its leakage of premium content.

With this data breach, the website owners secured the search server without problem of the future attacks. The only problem is for the people who are the users of that website, the hackers may use the information to blackmail the user and can provoke them they would be defamed to demand money from them. This is very dangerous than the information leak which may lead to may suicides. The information got by the hackers also contain the mail ids which are linked with the main data base and servers. If the hackers know about that details before the company could change all the credentials, then there would be a preferable and deep access to the information like personal photos of the users and the business information of the user like the status of the user in the society.

8. **Social Larks Data breach:**

Sociallarks is a foreign trading website/application. It is a trade marketing platform. The data breach took place in January,2021. The Sociallarks is a fast-growing media agency. The hugeness of the data leak is like the information of 200 million users is leaked. The leak is caused due to the verdict that the website handling server is not encrypted and is not a password protected one. This made the data leakage very easy. Anybody with the basic knowledge of the server IP address could easily access the data which is leaked. That is the problem raised here.

The size of the data is very huge and the data of the people like names, phone numbers, email addresses, profile descriptions, Linked In profile links who attached it, locations, connected social media links and account login names. It also can affect the user follower engagement data. The data is leaked for all the users who use the linked In, Instagram and Facebook users.

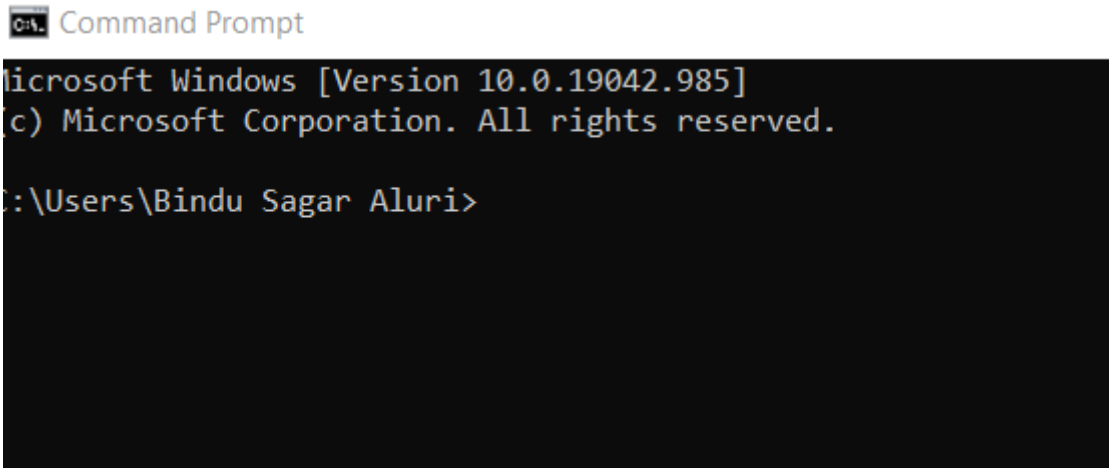
Windows Commands:

The commands are also called as shortcut keys. These are useful for direct accessing of the files and other information in the computer. The commands are also used for easy search of the file we want and open it. For a programmer or an ethical hacker, commands should be known as many as possible to save time. For a programmer or ethical hacker time is the most precious thing.

So, to learn some of the codes first follow the step:

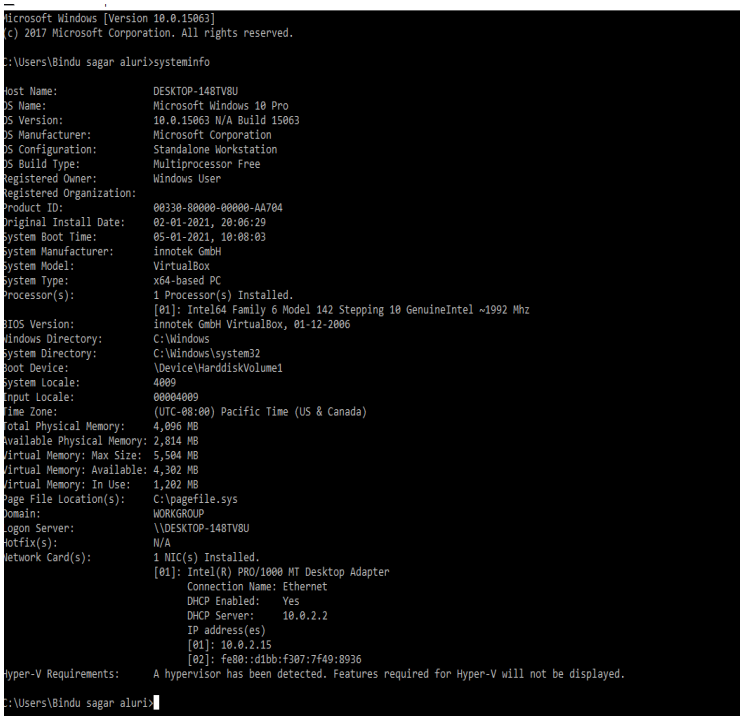
Open **'Windows Start' < cmd >**

Then we get a dialogue box like this as shown below.



1. Systeminfo:

Description: It gives all the information about the system.



2. ipconfig:

Description: It gives some info about IP configuration of the system.

```
C:\Users\Bindu sagar aluri>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d1bb:f307:7f49:8936%2
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2

C:\Users\Bindu sagar aluri>
```

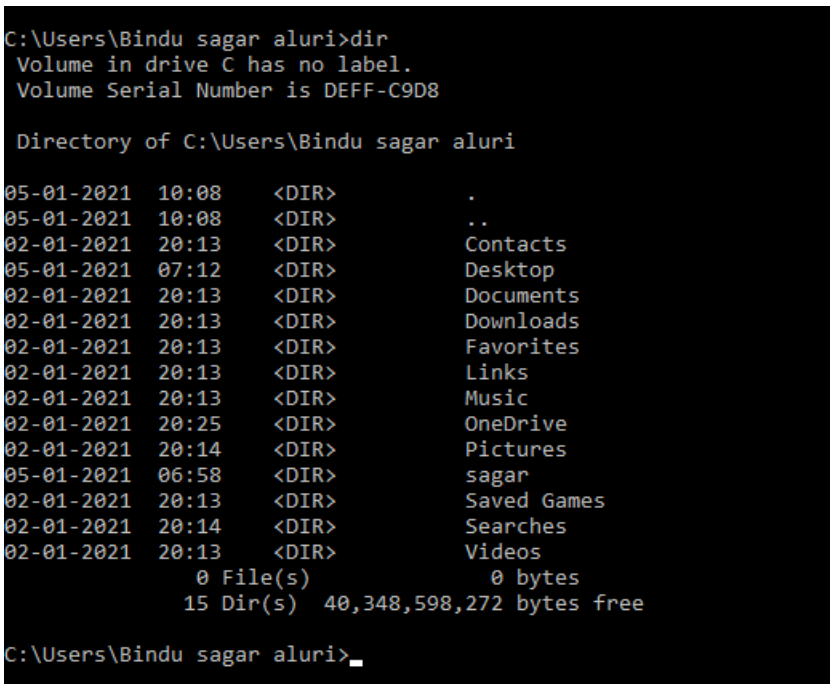
3. ipconfig/all:

Description: It gives all the configuration details of the system and total information in PC.

```
C:\Users\Bindu sagar aluri>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-148TV8U
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-45-AB-C9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d1bb:f307:7f49:8936%2(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.2.15(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 05 January 2021 10:08:12
   Lease Expires . . . . . . . . . . : 06 January 2021 10:08:18
   Default Gateway . . . . . . . . . : 10.0.2.2
   DHCP Server . . . . . . . . . . . : 10.0.2.2
   DHCPv6 IAID . . . . . . . . . . . : 50855975
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-82-FB-18-08-00-27-45-AB-C9
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Bindu sagar aluri>
```

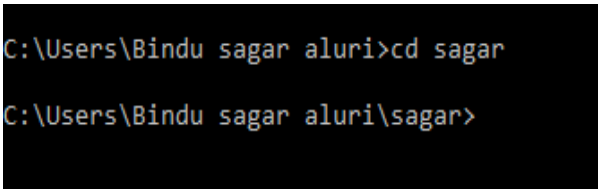
4. dir:

Description: It is used for listing all the files and also to navigate the files. It not only shows the list of the files but also shows the memory of the files.



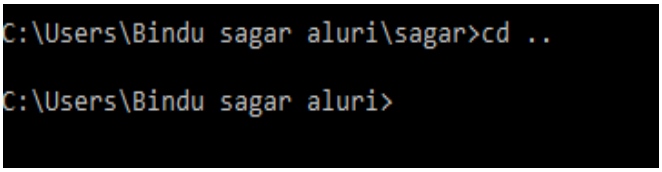
5. cd folder name:

Description: This command is used to change the current working directory and change to the directory created with the name ‘folder name’ given by us.



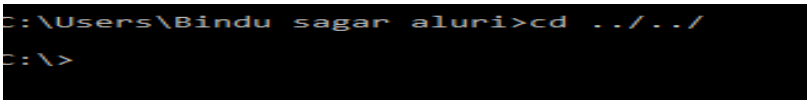
6. cd .. :

Description: It changes the present directory to the previous one.



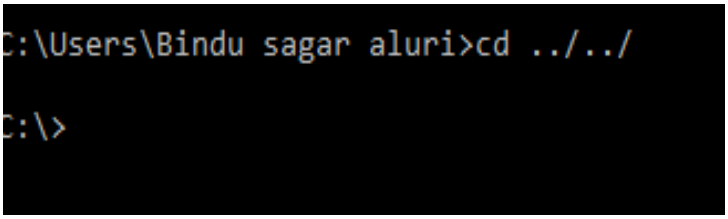
7. cd ../../ :

Description: It changes the current directory to the one before the previous directory.



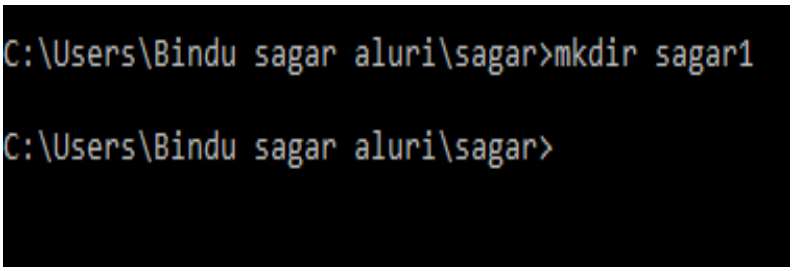
8. cd *address*:

Description: It changes the directory to the address given.



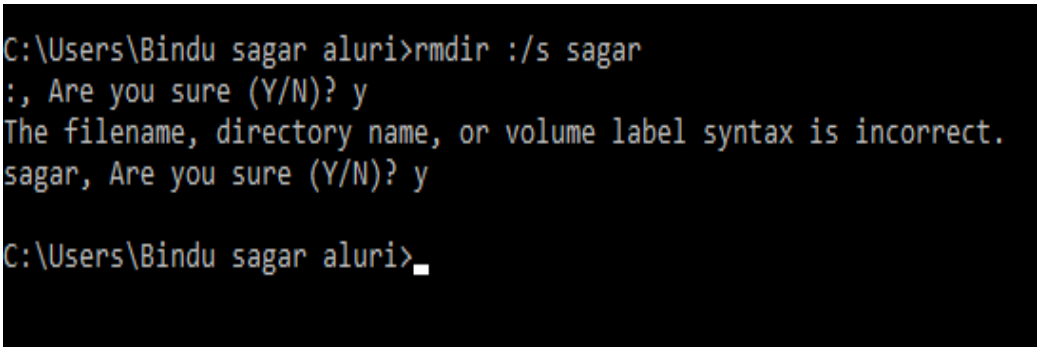
9. **mkdir folder name:**

Description: To create a new file in the directory. If needed space in the folder name, the whole thing must in double quotes.



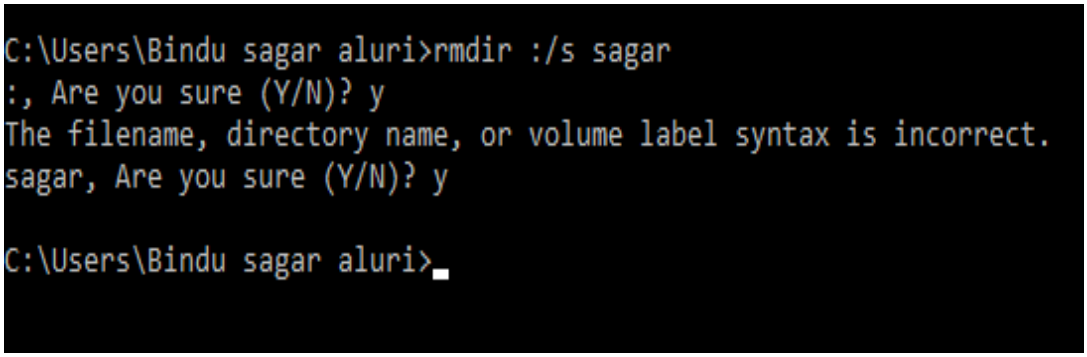
10. rmdir folder name:

Description: To remove the folder from the directory.



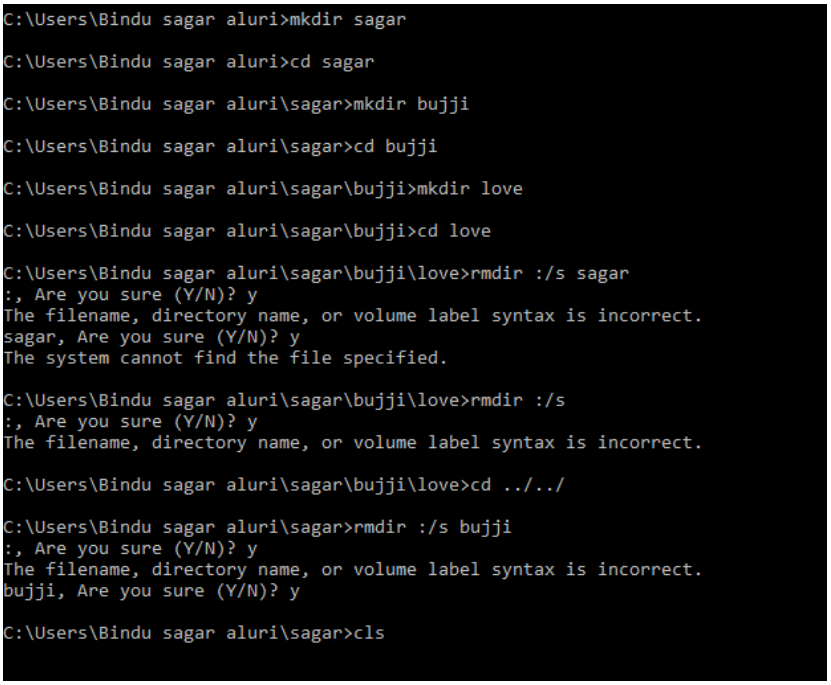
11. rmdir :/s folder name:

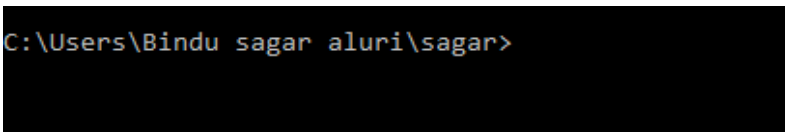
Description: To delete all the subfolders and directories on an address line.



12. cls:

Description: To clear the screen in command prompt.





13. color/? :

Description: To change the color of the command prompt in the front ground.

```
C:\Users\Bindu sagar aluri>color /?
Sets the default console foreground and background colors.

COLOR [attr]

  attr        Specifies color attribute of console output

Color attributes are specified by TWO hex digits -- the first
corresponds to the background; the second the foreground.  Each digit
can be any of the following values:

    0 = Black       8 = Gray
    1 = Blue        9 = Light Blue
    2 = Green       A = Light Green
    3 = Aqua        B = Light Aqua
    4 = Red         C = Light Red
    5 = Purple      D = Light Purple
    6 = Yellow      E = Light Yellow
    7 = White       F = Bright White

If no argument is given, this command restores the color to what it was
when CMD.EXE started.  This value either comes from the current console
window, the /T command line switch or from the DefaultColor registry
value.

The COLOR command sets ERRORLEVEL to 1 if an attempt is made to execute
the COLOR command with a foreground and background color that are the
same.

Example: "COLOR fc" produces light red on bright white

C:\Users\Bindu sagar aluri>
```

- To select the color, type ‘color<space>color number’, it changes the front ground color or text color.

```
C:\Users\Bindu sagar aluri>3
'3' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Bindu sagar aluri>color 3

C:\Users\Bindu sagar aluri>
```

- To change the background color, type ‘color<space>background color number front ground color number

```
C:\Users\Bindu sagar aluri>color 37

C:\Users\Bindu sagar aluri>
```

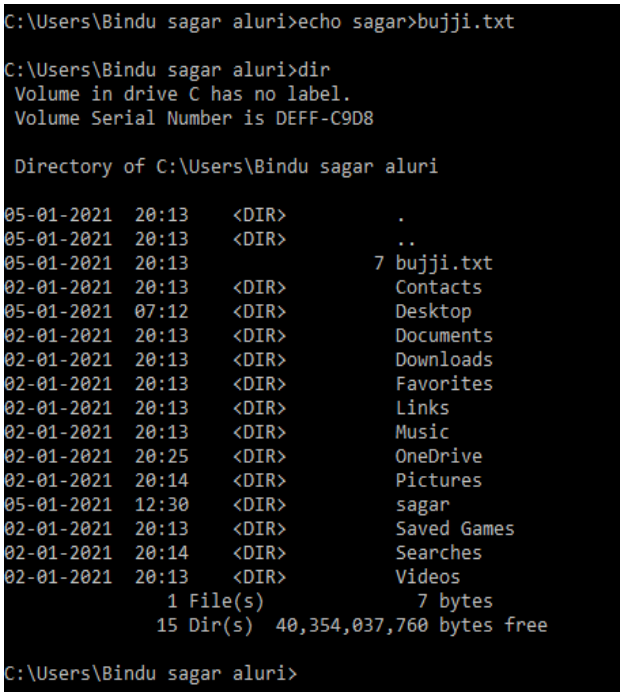
14. echo name:

Description: It displays/prints the name typed. It is the same function as ‘printf’ in C.

```
C:\Users\Bindu sagar aluri>echo sagar
sagar
```

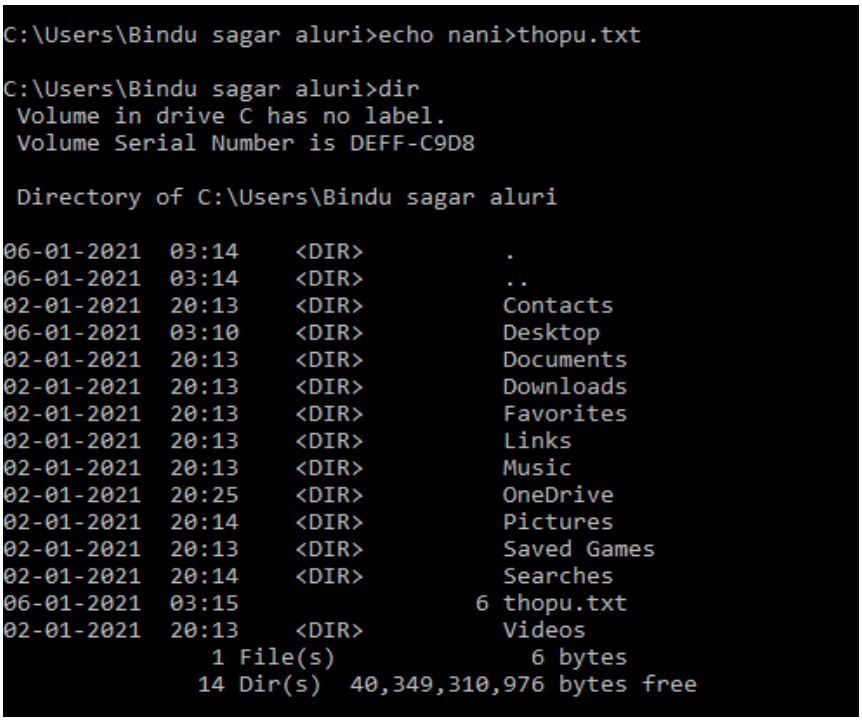
15. echo text > filename.txt :

Description: It creates a file with the filename given and inserts the text in it.



16. echo text > *address*:

Description: It displays the text in the specified filename given by creating it.



17. echo text >> *address*:

Description: It adds the data to the file without replacing the previous ones.

```
C:\Users\Bindu sagar aluri>echo sagar
sagar
```

```
C:\Users\Bindu sagar aluri>echo sagar>>thopu.txt

C:\Users\Bindu sagar aluri>
```

18. type filename.txt:

Description: To display the text in specific file.

```
C:\Users\Bindu sagar aluri\Documents>type thopu.txt
sagar

C:\Users\Bindu sagar aluri\Documents>
```

19. copy filename.txt location:

Description: To copy a file from one location to the other.

```
C:\Users\Bindu sagar aluri\Documents>copy thopu.txt c:\users\public\publicdocuments
        1 file(s) copied.

C:\Users\Bindu sagar aluri\Documents>
```

20. del filename.txt:

Description: To delete the data in the file.

```
C:\Users\Bindu sagar aluri>del thopu.txt

C:\Users\Bindu sagar aluri>dir
 Volume in drive C has no label.
 Volume Serial Number is DEFF-C9D8

 Directory of C:\Users\Bindu sagar aluri

06-01-2021  03:24    <DIR>          .
06-01-2021  03:24    <DIR>          ..
02-01-2021  20:13    <DIR>          Contacts
06-01-2021  03:10    <DIR>          Desktop
02-01-2021  20:13    <DIR>          Documents
02-01-2021  20:13    <DIR>          Downloads
02-01-2021  20:13    <DIR>          Favorites
02-01-2021  20:13    <DIR>          Links
02-01-2021  20:13    <DIR>          Music
02-01-2021  20:25    <DIR>          OneDrive
02-01-2021  20:14    <DIR>          Pictures
02-01-2021  20:13    <DIR>          Saved Games
02-01-2021  20:14    <DIR>          Searches
02-01-2021  20:13    <DIR>          Videos
               0 File(s)              0 bytes
              14 Dir(s)  40,349,319,168 bytes free

C:\Users\Bindu sagar aluri>
```

21. move filename.txt location:

Description: To move file from one location to the other.

```
C:\Users\Bindu sagar aluri\Documents>move thopu.txt desktop
       1 file(s) moved.

C:\Users\Bindu sagar aluri\Documents>
```

22. attrib +h filename.txt:

Description: To hide a file.

```
C:\Users\Bindu sagar aluri\Documents>attrib +h thopu.txt

C:\Users\Bindu sagar aluri\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is DEFF-C9D8

 Directory of C:\Users\Bindu sagar aluri\Documents

06-01-2021  04:02    <DIR>          .
06-01-2021  04:02    <DIR>          ..
06-01-2021  03:28                 7 desktop
               1 File(s)              7 bytes
               2 Dir(s)  40,344,055,808 bytes free

C:\Users\Bindu sagar aluri\Documents>
```

23. attrib -h filename.txt:

Description: To unhide the hided file.

```
C:\Users\Bindu sagar aluri\Documents>attrib -h thopu.txt

C:\Users\Bindu sagar aluri\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is DEFF-C9D8

 Directory of C:\Users\Bindu sagar aluri\Documents

06-01-2021  04:02    <DIR>          .
06-01-2021  04:02    <DIR>          ..
06-01-2021  03:28                 7 desktop
06-01-2021  04:02                15 thopu.txt
               2 File(s)             22 bytes
               2 Dir(s)  40,343,732,224 bytes free

C:\Users\Bindu sagar aluri\Documents>
```

24. tasklist:

Description: To display all the tasks done in background as well as front ground.

```
C:\Users\Bindu sagar aluri\Documents>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        124 K
smss.exe                       316 Services                   0      1,160 K
csrss.exe                      412 Services                   0      5,048 K
wininit.exe                    496 Services                   0      6,272 K
csrss.exe                      504 Console                    1      4,576 K
winlogon.exe                   596 Console                    1      9,368 K
services.exe                   648 Services                   0      8,164 K
lsass.exe                      656 Services                   0     12,280 K
fontdrvhost.exe                756 Console                    1      4,852 K
fontdrvhost.exe                752 Services                   0      3,432 K
svchost.exe                    768 Services                   0      3,740 K
svchost.exe                    844 Services                   0     22,664 K
svchost.exe                    896 Services                   0     10,204 K
svchost.exe                    944 Services                   0      6,212 K
dwm.exe                         72 Console                    1     75,012 K
svchost.exe                    416 Services                   0      7,248 K
svchost.exe                    864 Services                   0      9,004 K
svchost.exe                   1036 Services                   0     18,264 K
svchost.exe                   1044 Services                   0     10,628 K
svchost.exe                   1052 Services                   0      5,368 K
```

25. notepad:

Description: To open notepad.

```
C:\Users\Bindu sagar aluri\Documents>notepad
```

26. filename.txt:

Description: To open the needed file or filename given.

```
C:\Users\Bindu sagar aluri\Documents>thopu.txt
```

27. taskKill/IM notepad.exe:

Description: To stop the tasks running in the background.

```
C:\Users\Bindu sagar aluri\Documents>taskKill/IM Notepad.exe
SUCCESS: Sent termination signal to the process "notepad.exe" with PID 3860.
```

28. call:

Description: It calls a batch file from another one.

```
C:\Users\Bindu sagar aluri\Documents>call
```

29. ping:

Description: It shows the ping of the system

```
C:\Users\Bindu sagar aluri\Documents>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

30. pathping:

Description: It shows the path of the ping of the system.

```
C:\Users\Bindu sagar aluri\Documents>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.
```

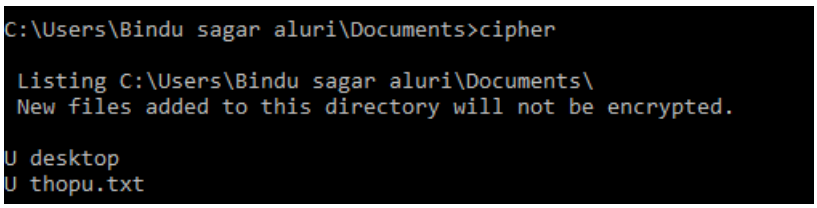
31. assoc:

Description: It shows the meaning of the file associated with it.

```
C:\Users\Bindu sagar aluri\Documents>assoc.txt
.txt=txtfile
```

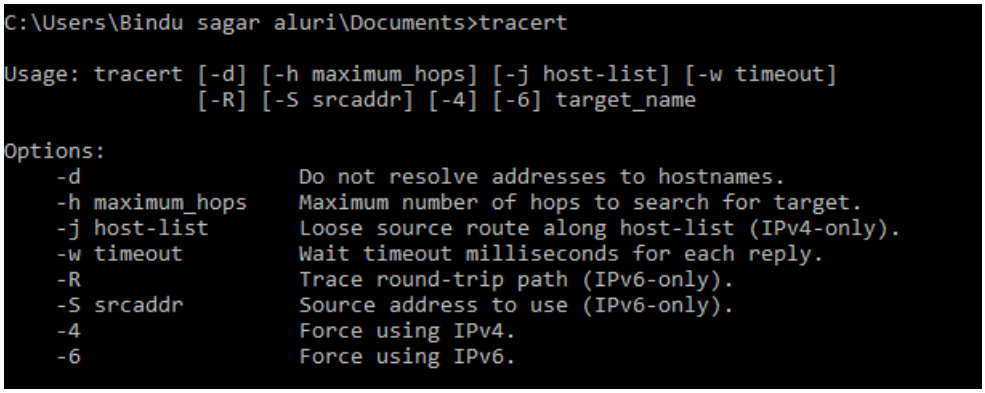
32. cipher:

Description: It wipes out all the undeleted files which are not useful at all and it is the one which directly wipes out all the files of the directory easily



33. Tracert:

Description: If we type the tracert followed by the target device IP address, we can trace the information about each step in the route between the system and target.



34. driverquery:

Description: It gives access to a list of what are the drivers in the system.

```
C:\Users\Bindu sagar aluri\Documents>driverquery

Module Name  Display Name           Driver Type   Link Date
============ ====================== ============= ====================
1394ohci     1394 OHCI Compliant Ho Kernel        10-12-2006 13:44:38
3ware        3ware                  Kernel        18-05-2015 15:28:03
ACPI         Microsoft ACPI Driver  Kernel        09-12-1975 03:17:08
AcpiDev      ACPI Devices driver    Kernel        07-12-1993 03:22:19
acpiex       Microsoft ACPIEx Drive Kernel        01-03-2087 05:53:50
acpipagr     ACPI Processor Aggrega Kernel        24-01-2081 05:36:36
AcpiPmi      ACPI Power Meter Drive Kernel        19-11-2006 18:20:15
acpitime     ACPI Wake Alarm Driver Kernel        09-02-1974 04:10:30
ADP80XX      ADP80XX                Kernel        09-04-2015 13:49:48
AFD          Ancillary Function Dri Kernel        25-03-2096 09:36:43
ahcache      Application Compatibil Kernel        28-07-2004 21:52:50
AmdK8        AMD K8 Processor Drive Kernel        16-06-2040 00:17:43
AmdPPM       AMD Processor Driver   Kernel        23-12-2077 13:48:10
amdsata      amdsata                Kernel        14-05-2015 05:14:52
amdsbs       amdsbs                 Kernel        11-12-2012 13:21:44
amdxata      amdxata                Kernel        30-04-2015 17:55:35
AppID        AppID Driver           Kernel        17-03-2072 17:13:51
applockerflt Smartlocker Filter Dri Kernel        17-09-2101 02:17:41
AppvStrm     AppvStrm               File System   30-11-2078 01:40:53
AppvVemgr    AppvVemgr              File System   29-04-2039 02:17:05
AppvVfs      AppvVfs                File System   19-04-2058 12:11:18
arcsas       Adaptec SAS/SATA-II RA Kernel        09-04-2015 12:12:07
AsyncMac     RAS Asynchronous Media Kernel        08-08-2097 07:12:49
atapi        IDE Channel            Kernel        27-11-2000 15:57:51
b06bdrv      QLogic Network Adapter Kernel        25-05-2016 00:03:08
BasicDisplay BasicDisplay           Kernel        22-02-2093 07:33:08
BasicRender  BasicRender            Kernel        04-04-2070 11:19:55
bcmfn2       bcmfn2 Service         Kernel        31-10-2016 19:09:15
Beep         Beep                   Kernel        01-01-2060 08:27:10
bowser       Browser Support Driver File System   14-11-2063 14:49:42
BthAvrcpTg   Bluetooth Audio/Video  Kernel        11-09-2022 12:32:06
BthHFEnum    Bluetooth Hands-Free A Kernel        18-04-2004 21:32:55
bthhfhid     Bluetooth Hands-Free C Kernel        24-04-2011 21:21:49
```

35. driverquery -v:

Description: The driverquery is extended to driverquery -v to get access to complete drivers list in the system.

```
C:\Users\Bindu sagar aluri\Documents>driverquery -v

Module Name  Display Name           Description            Driver Type  Start Mode State    Status  Accept Stop Accept Pause Paged Pool(bytes) Code(bytes) BSS(bytes) Link Date            Path                                          Init(bytes)
============ ====================== ====================== ============ ========== ========= ======= =========== ============ ================ ============ ========== ==================== ============================================= ============
1394ohci     1394 OHCI Compliant Ho 1394 OHCI Compliant Ho Kernel       Manual     Stopped   OK      FALSE       FALSE        4,096            2,04,800     0          10-12-2006 13:44:38  C:\Windows\system32\drivers\1394ohci.sys      4,096
3ware        3ware                  3ware                  Kernel       Manual     Stopped   OK      FALSE       FALSE        0                81,920       0          18-05-2015 15:28:03  C:\Windows\system32\drivers\3ware.sys         4,096
ACPI         Microsoft ACPI Driver  Microsoft ACPI Driver  Kernel       Boot       Running   OK      TRUE        FALSE        1,55,648         4,05,504     0          09-12-1975 03:17:08  C:\Windows\system32\drivers\ACPI.sys          24,576
AcpiDev      ACPI Devices driver    ACPI Devices driver    Kernel       Manual     Stopped   OK      FALSE       FALSE        8,192            8,192        0          07-12-1993 03:22:19  C:\Windows\system32\drivers\AcpiDev.sys       4,096
acpiex       Microsoft ACPIEx Drive Microsoft ACPIEx Drive Kernel       Boot       Running   OK      TRUE        FALSE        36,864           61,440       0          01-03-2087 05:53:50  C:\Windows\system32\Drivers\acpiex.sys        4,096
acpipagr     ACPI Processor Aggrega ACPI Processor Aggrega Kernel       Manual     Stopped   OK      FALSE       FALSE        4,096            4,096        0          24-01-2081 05:36:36  C:\Windows\system32\drivers\acpipagr.sys      4,096
AcpiPmi      ACPI Power Meter Drive ACPI Power Meter Drive Kernel       Manual     Stopped   OK      FALSE       FALSE        8,192            4,096        0          19-11-2006 18:20:15  C:\Windows\system32\drivers\acpipmi.sys       4,096
acpitime     ACPI Wake Alarm Driver ACPI Wake Alarm Driver Kernel       Manual     Stopped   OK      FALSE       FALSE        8,192            4,096        0          09-02-1974 04:10:30  C:\Windows\system32\drivers\acpitime.sys      4,096
ADP80XX      ADP80XX                ADP80XX                Kernel       Manual     Stopped   OK      FALSE       FALSE        0                11,01,824    0          09-04-2015 13:49:48  C:\Windows\system32\drivers\ADP80XX.SYS       4,096
AFD          Ancillary Function Dri Ancillary Function Dri Kernel       System     Running   OK      TRUE        FALSE        3,23,584         1,18,784     0          25-03-2096 09:36:43  C:\Windows\system32\drivers\afd.sys           8,192
```

36. Netstat:

Description: It displays the list of all open ports in the present system.

```
C:\Users\Bindu sagar aluri\Documents>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
```

37. powercfg:

Description: It is used to know how the system uses energy.

```
C:\Users\Bindu sagar aluri\Documents>powercfg /?

POWERCFG /COMMAND [ARGUMENTS]

Description:
  Enables users to control power settings on a local system.

  For detailed command and option information, run "POWERCFG /? <COMMAND>"

Command List:
  /LIST, /L           Lists all power schemes.

  /QUERY, /Q          Displays the contents of a power scheme.

  /CHANGE, /X         Modifies a setting value in the current power scheme.

  /CHANGENAME         Modifies the name and description of a power scheme.

  /DUPLICATESCHEME    Duplicates a power scheme.

  /DELETE, /D         Deletes a power scheme.

  /DELETESETTING      Deletes a power setting.

  /SETACTIVE, /S      Makes a power scheme active on the system.

  /GETACTIVESCHEME    Retrieves the currently active power scheme.

  /SETACVALUEINDEX    Sets the value associated with a power setting
                      while the system is powered by AC power.

  /SETDCVALUEINDEX    Sets the value associated with a power setting
                      while the system is powered by DC power.

  /IMPORT             Imports all power settings from a file.

  /EXPORT             Exports a power scheme to a file.

  /ALIASES            Displays all aliases and their corresponding GUIDs.
```

38. powercfg hibernate on:

Description: It is used to on the hibernation.

```
C:\Users\Bindu sagar aluri\Documents>powercfg hibernate on
Hibernation failed with the following error: The request is not supported.

The following items are preventing hibernation on this system.
        The system firmware does not support hibernation.
```

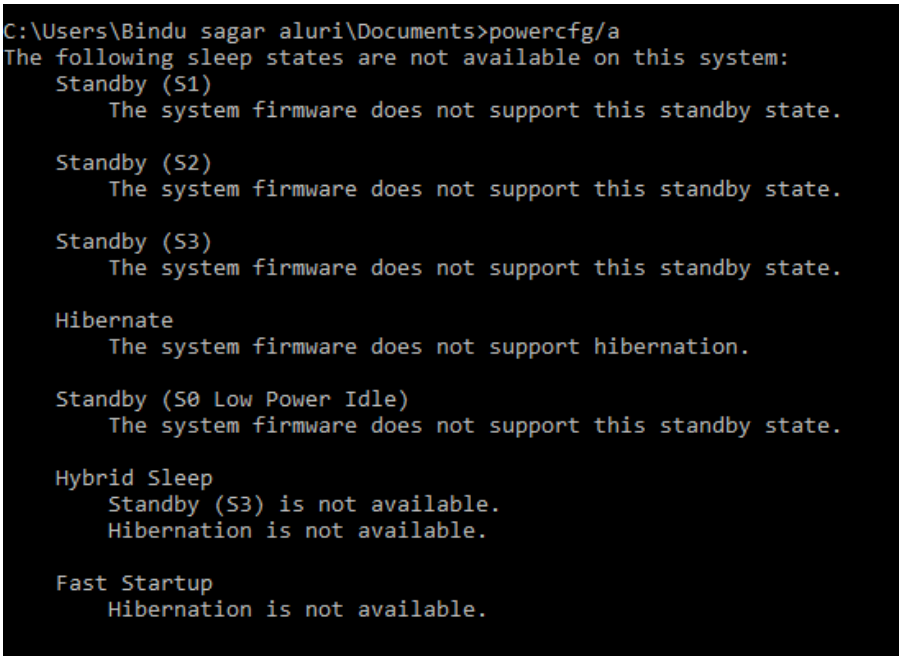
39. powercfg hibernation off:

Description: It is used to off the hibernation

```
C:\Users\Bindu sagar aluri\Documents>powercfg hibernate off
Hibernation failed with the following error: A required privilege is not held by the client.

The following items are preventing hibernation on this system.
        The system firmware does not support hibernation.
```

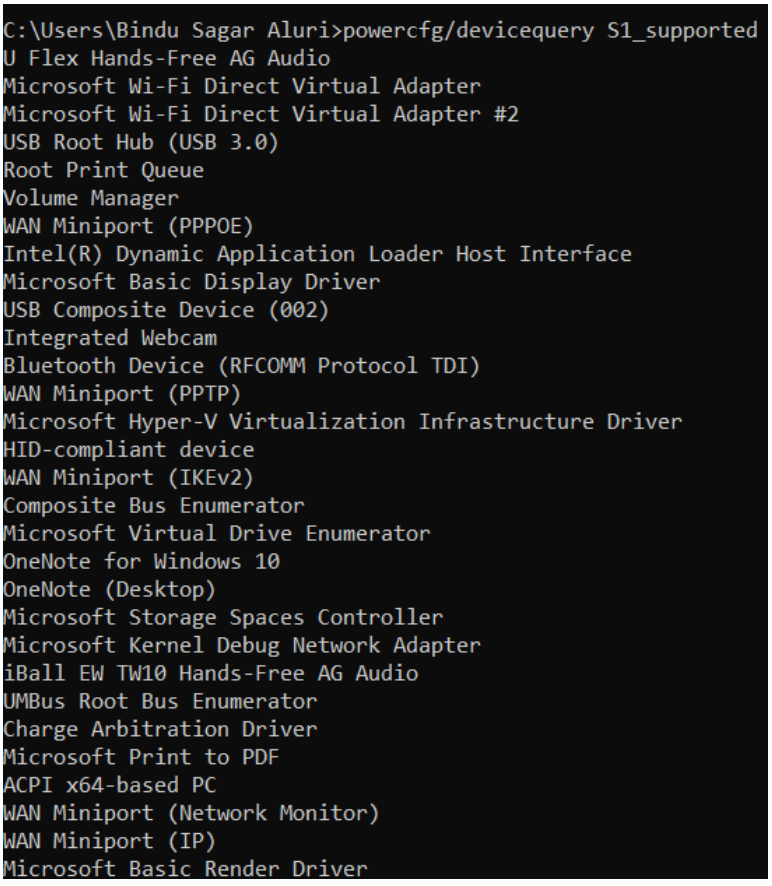
40. powercfg/a:

Description: It is used to view the power saving states available in the system



41. powercfg/devicequery s1_supported:

Description: It is which displays a list of devices on the system that support connected standby.



42. powercfg/lastwake:

Description: It shows us what device last woke the system from a sleep state.

```
C:\Users\Bindu sagar aluri\Documents>powercfg/lastwake
Wake History Count - 0
```

43. shutdown:

Description: It shuts down the system.

```
C:\Users\Bindu sagar aluri\Documents>shutdown
```

44. shutdown/r/o:

Description: It restarts the system.

```
C:\Users\Bindu sagar aluri\Documents>shutdown/r/o
```

45. tasklist -m:

Description: It locates all the DLL files associated with the active files in the system.

```
C:\Users\Bindu sagar aluri\Documents>tasklist -m

Image Name                     PID Modules
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       316 N/A
csrss.exe                      412 N/A
wininit.exe                    496 N/A
csrss.exe                      504 N/A
winlogon.exe                   596 N/A
services.exe                   648 N/A
lsass.exe                      656 N/A
fontdrvhost.exe                756 N/A
fontdrvhost.exe                752 N/A
svchost.exe                    768 N/A
svchost.exe                    844 N/A
svchost.exe                    896 N/A
svchost.exe                    944 N/A
dwm.exe                         72 N/A
svchost.exe                    864 N/A
svchost.exe                   1036 N/A
svchost.exe                   1044 N/A
svchost.exe                   1052 N/A
svchost.exe                   1108 N/A
svchost.exe                   1160 N/A
svchost.exe                   1220 N/A
svchost.exe                   1276 N/A
svchost.exe                   1332 N/A
svchost.exe                   1372 N/A
```

46. chkdsk:

Description: It scans the disk immediately

```
C:\Users\Bindu sagar aluri\Documents>chkdsk
Access Denied as you do not have sufficient privileges.
You have to invoke this utility running in elevated mode.
```

47. cmd:

Description: To start the command prompt.

```
C:\Users\Bindu sagar aluri\Documents>cmd
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.
```

48. time:

Description: It displays the time in the system.

```
C:\Users\Bindu sagar aluri\Documents>time
The current time is:  4:19:19.63
```

49. cd:

Description: It displays the folder that we are currently in.

```
C:\Users\Bindu sagar aluri\sagar>cd ..

C:\Users\Bindu sagar aluri>
```

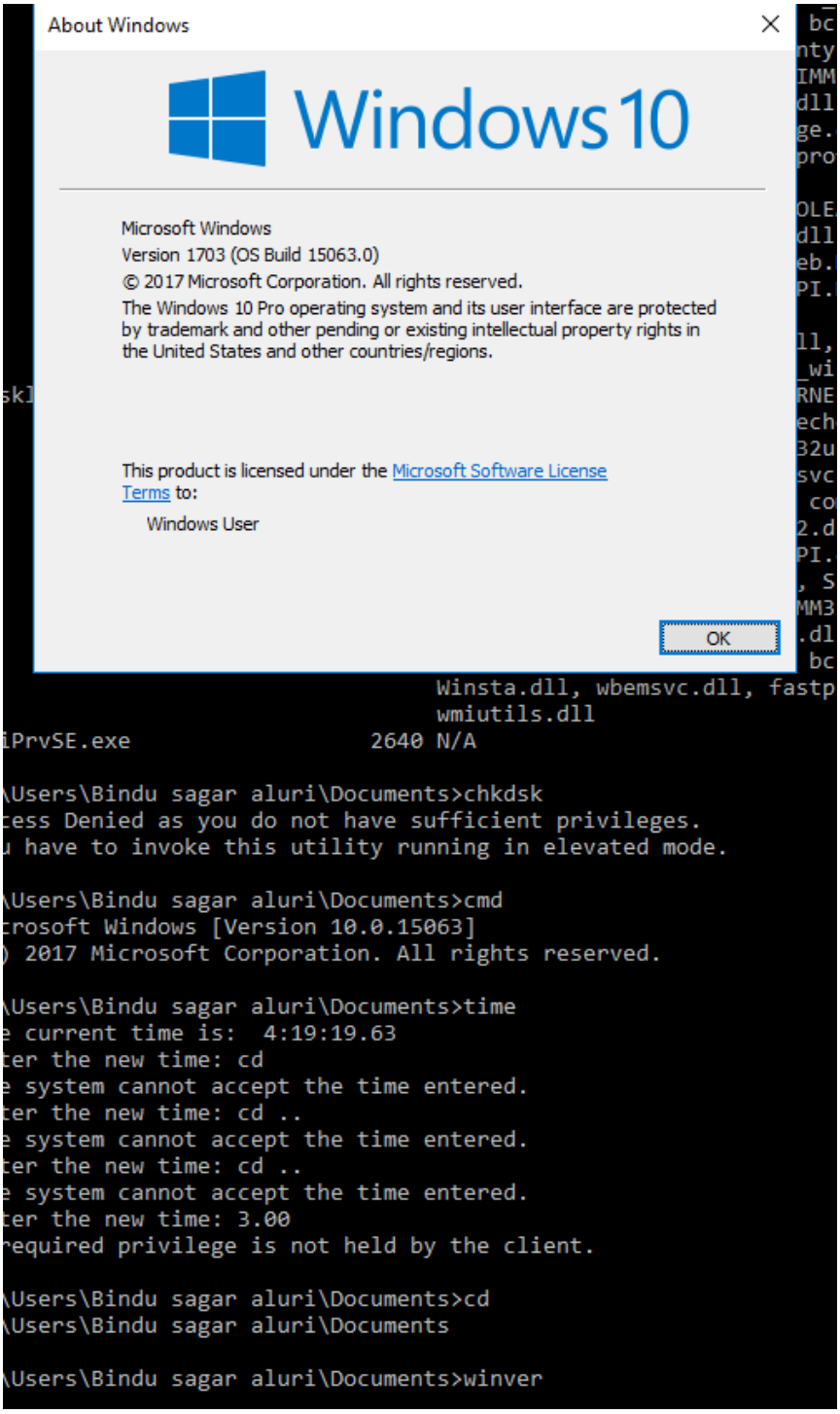
50. clip /?:

Description: It redirects the output from any command to the clipboard in windows.

```
C:\Users\Bindu Sagar Aluri>clip/?

CLIP

Description:
    Redirects output of command line tools to the Windows clipboard.
    This text output can then be pasted into other programs.

Parameter List:
    /?                  Displays this help message.

Examples:
    DIR | CLIP          Places a copy of the current directory
                        listing into the Windows clipboard.

    CLIP < README.TXT   Places a copy of the text from readme.txt
                        on to the Windows clipboard.
```

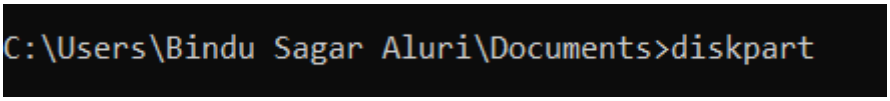
51. winver:

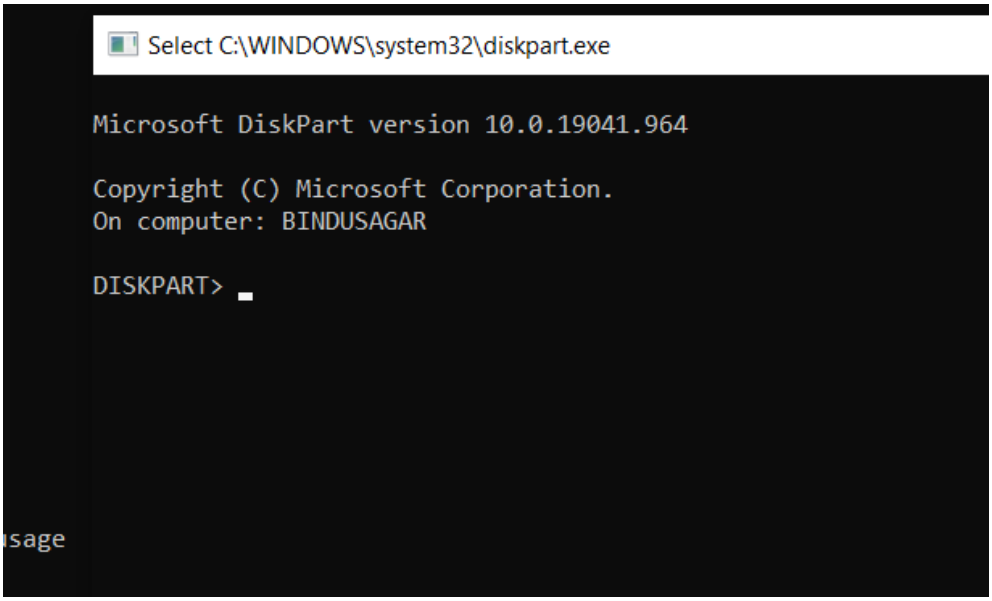
Description: It shows the windows version



52. diskpart:

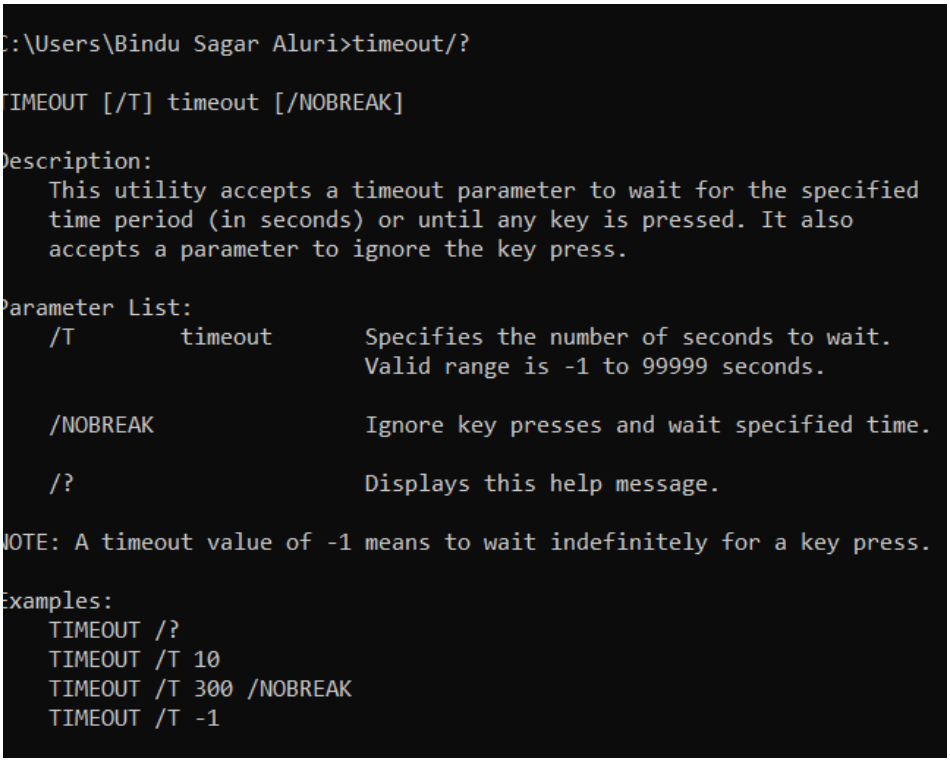
Description: It manages the volume and opens and new tab of diskpart.





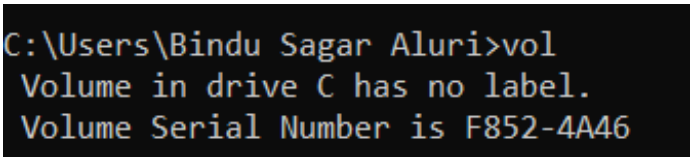
53. timeout /?:

Description: It is used to provide a specific timeout value during a procedure.



54. vol:

Description: displays the label and serial number of a drive.



55. robocopy:

Description: This is an extension of copy and xcopy. It is possible to transfer data successfully even if there are interruptions in the network.

```
C:\Users\Bindu Sagar Aluri>robocopy

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : 17 May 2021 13:50:18
       Simple Usage :: ROBOCOPY source destination /MIR

            source :: Source Directory (drive:\path or \\server\share\path).
       destination :: Destination Dir  (drive:\path or \\server\share\path).
             /MIR :: Mirror a complete directory tree.

    For more usage information run ROBOCOPY /?


****  /MIR can DELETE files as well as copy them !

C:\Users\Bindu Sagar Aluri>undelete
'undelete' is not recognized as an internal or external command,
operable program or batch file.
```

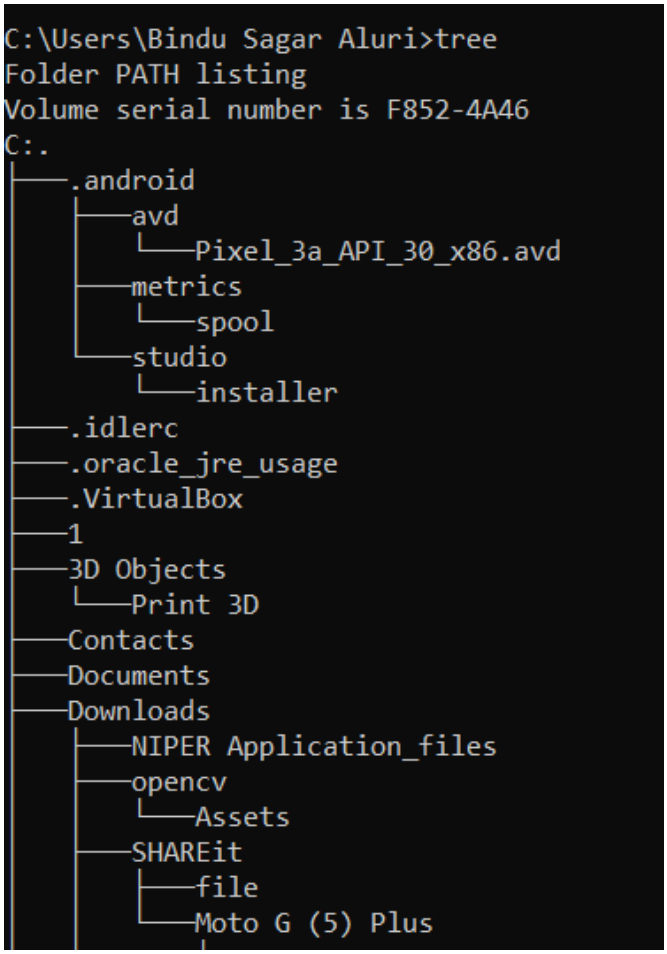
56. cacls:

Description: display or modify the access control lists for files and folders.

```
C:\Users\Bindu Sagar Aluri>cacls

NOTE: Cacls is now deprecated, please use Icacls.

Displays or modifies access control lists (ACLs) of files

CACLS filename [/T] [/M] [/L] [/S[:SDDL]] [/E] [/C] [/G user:perm]
       [/R user [...]] [/P user:perm [...]] [/D user [...]]
   filename      Displays ACLs.
   /T            Changes ACLs of specified files in
                 the current directory and all subdirectories.
   /L            Work on the Symbolic Link itself versus the target
   /M            Changes ACLs of volumes mounted to a directory
   /S            Displays the SDDL string for the DACL.
   /S:SDDL       Replaces the ACLs with those specified in the SDDL string
                 (not valid with /E, /G, /R, /P, or /D).
   /E            Edit ACL instead of replacing it.
   /C            Continue on access denied errors.
   /G user:perm  Grant specified user access rights.
                 Perm can be: R  Read
                              W  Write
                              C  Change (write)
                              F  Full control
```

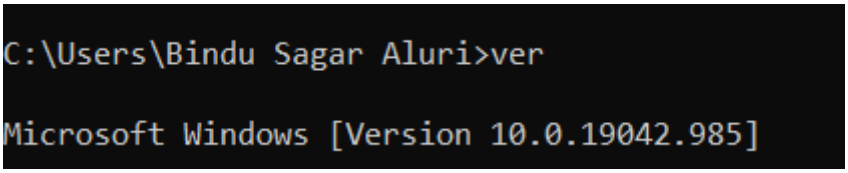
57. tree:

Description: graphically displace the directory structure of a driver or path.



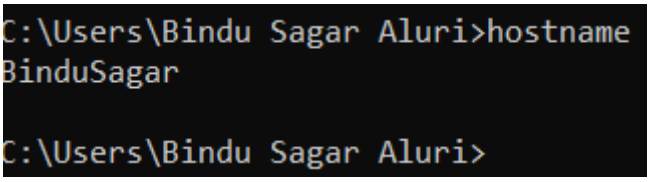
58. ver:

Description: displays the current version of the windows in the system sing the cmd.



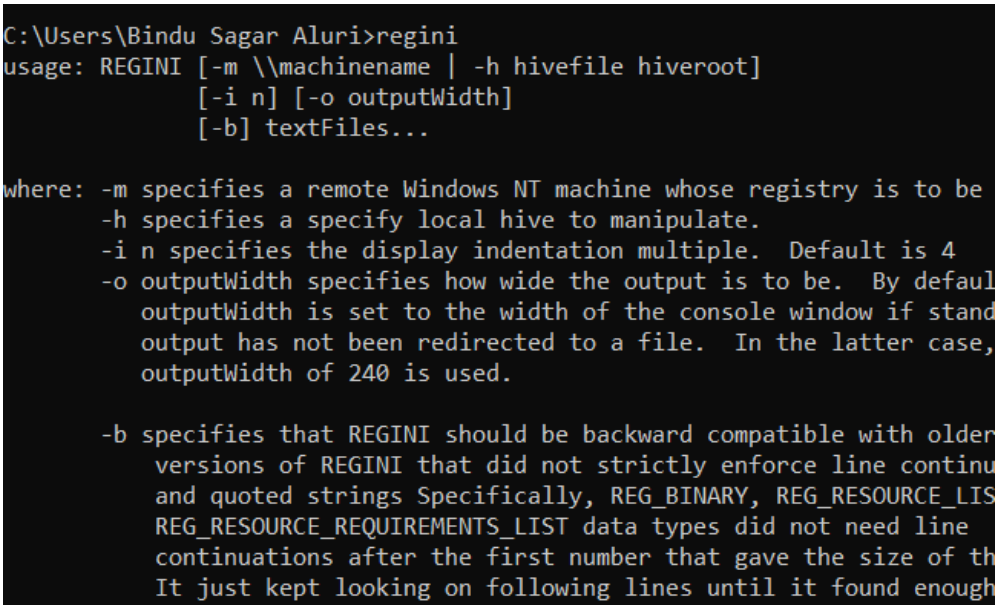
59. hostname:

Description: It displays the hostname.



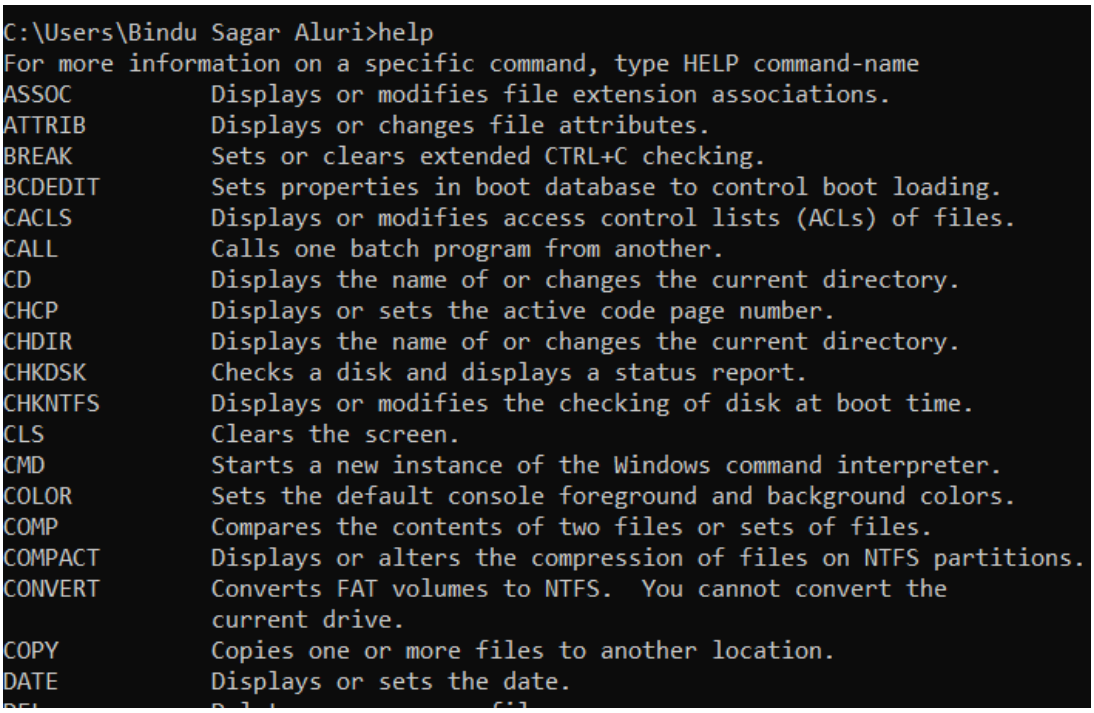
60. regini:

Description: changes registry authorizations.



61. help:

Description: It displays the help information for the windows commands.

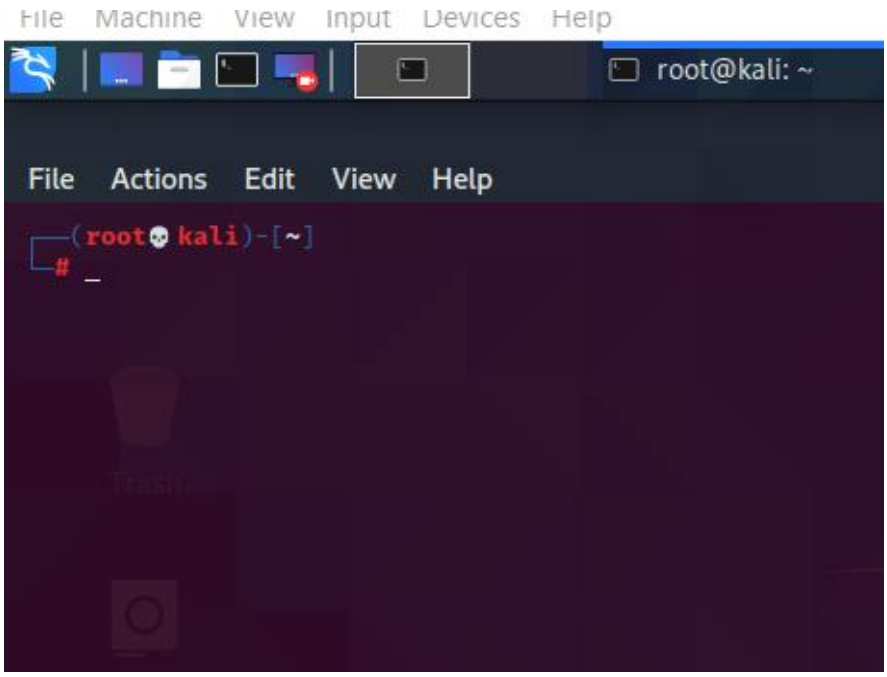


Linux commands:

The Linux commands are the shortcut keys for the operations in the Linux terminals. These must be known by the ethical hackers for fastness in the work. To save time and to increase the efficiency, the Linux commands must be learnt.

To learn some of the codes first open the **"Linux terminal"**.

We can see a terminal as shown below.



1. uname -a:

Description: It displays the name of the Linux.

```
(root kali)-[~]
# uname -a
Linux kali 5.9.0-kali1-amd64 #1 SMP Debian 5.9.1-1kali2 (2020-10-29) x86_64 GNU/Linux
```

2. uptime:

Description: To see the present time.

```
(root kali)-[~]
# uptime
07:42:35 up  1:32,  1 user,  load average: 0.19, 0.19, 0.14
```

3. hostname:

Description: To see the name of the host.

```
(root kali)-[~]
# hostname
kali
```

4. uname –help:

Description: It prints certain system information.

```
┌──(root💀kali)-[~]
└─# uname --help
Usage: uname [OPTION]...
Print certain system information.  With no OPTION, same as -s.

  -a, --all                print all information, in the following order,
                             except omit -p and -i if unknown:
  -s, --kernel-name        print the kernel name
  -n, --nodename           print the network node hostname
  -r, --kernel-release     print the kernel release
  -v, --kernel-version     print the kernel version
  -m, --machine            print the machine hardware name
  -p, --processor          print the processor type (non-portable)
  -i, --hardware-platform  print the hardware platform (non-portable)
  -o, --operating-system   print the operating system
      --help     display this help and exit
      --version  output version information and exit

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/uname>
or available locally via: info '(coreutils) uname invocation'
```

5. last reboot:

Description: The last date on which the system is rebooted.

```
┌──(root💀kali)-[~]
└─# last reboot
reboot   system boot  5.9.0-kali1-amd6 Sun Jan 10 06:10   still running
reboot   system boot  5.9.0-kali1-amd6 Sat Jan  9 13:34   still running
reboot   system boot  5.9.0-kali1-amd6 Sat Jan  9 08:21   still running
reboot   system boot  5.9.0-kali1-amd6 Sat Jan  9 08:16   still running
reboot   system boot  5.9.0-kali1-amd6 Sat Jan  9 08:14   still running
reboot   system boot  5.9.0-kali1-amd6 Sat Jan  9 08:12   still running
reboot   system boot  5.9.0-kali1-amd6 Tue Nov 17 09:12 - 09:47  (00:34)

wtmp begins Tue Nov 17 09:12:38 2020
```

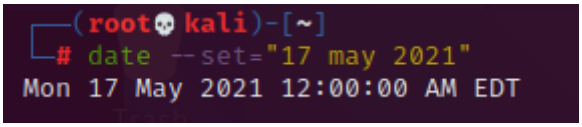
6. date:

Description: It displays the date of the system.

```
┌──(root💀kali)-[~]
└─# date
Mon 17 May 2021 07:32:37 AM EDT

┌──(root💀kali)-[~]
└─# _
```

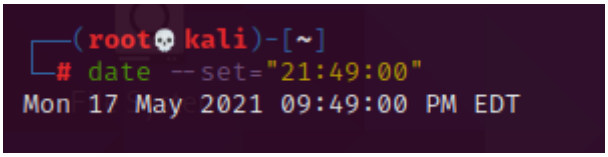
7. date –set:

Description: It is used to set or alter the date in the system.



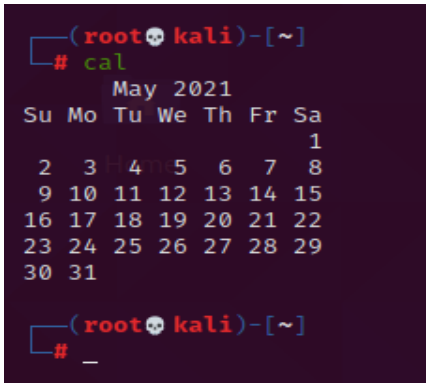
8. date –set:

Description: To set time in the system.



9. cal:

Description: To display the calendar.

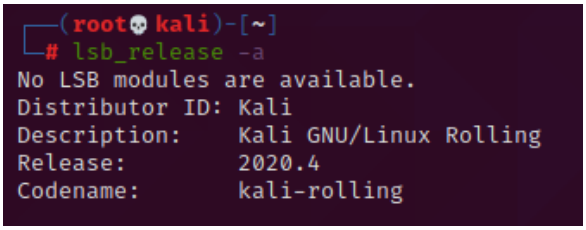


10. whoami:

Description: To see the username.

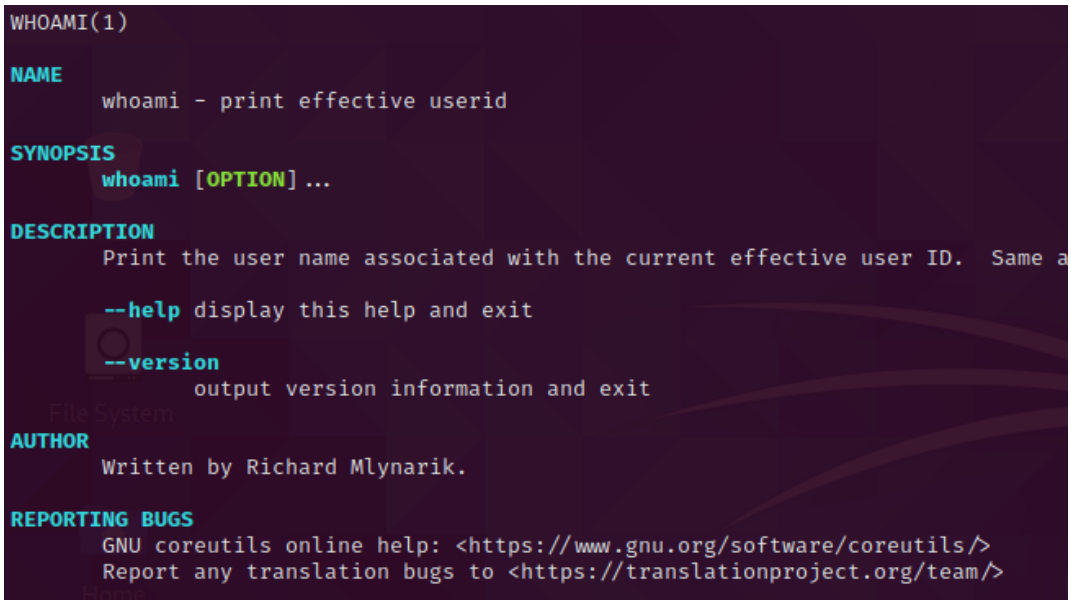
11. lsb_release -a:

Description: version of the Linux is installed



12. man whoami:

Description: To see all the information of the specified command.

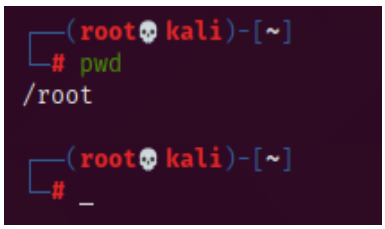


13. cd:

Description: To move from one directory to the other.

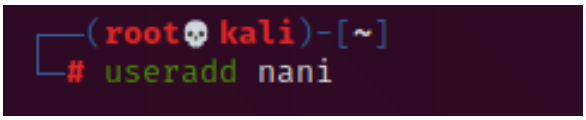
14. pwd:

Description: present working directory.



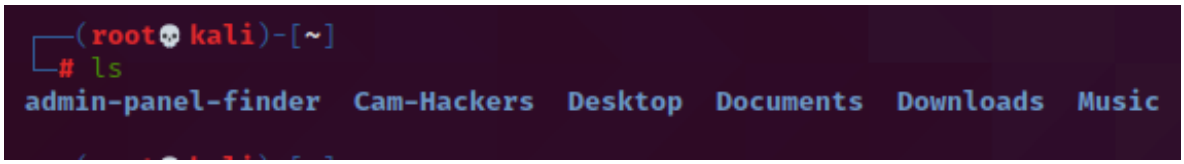
15. useradd name:

Description: To create a new user account.



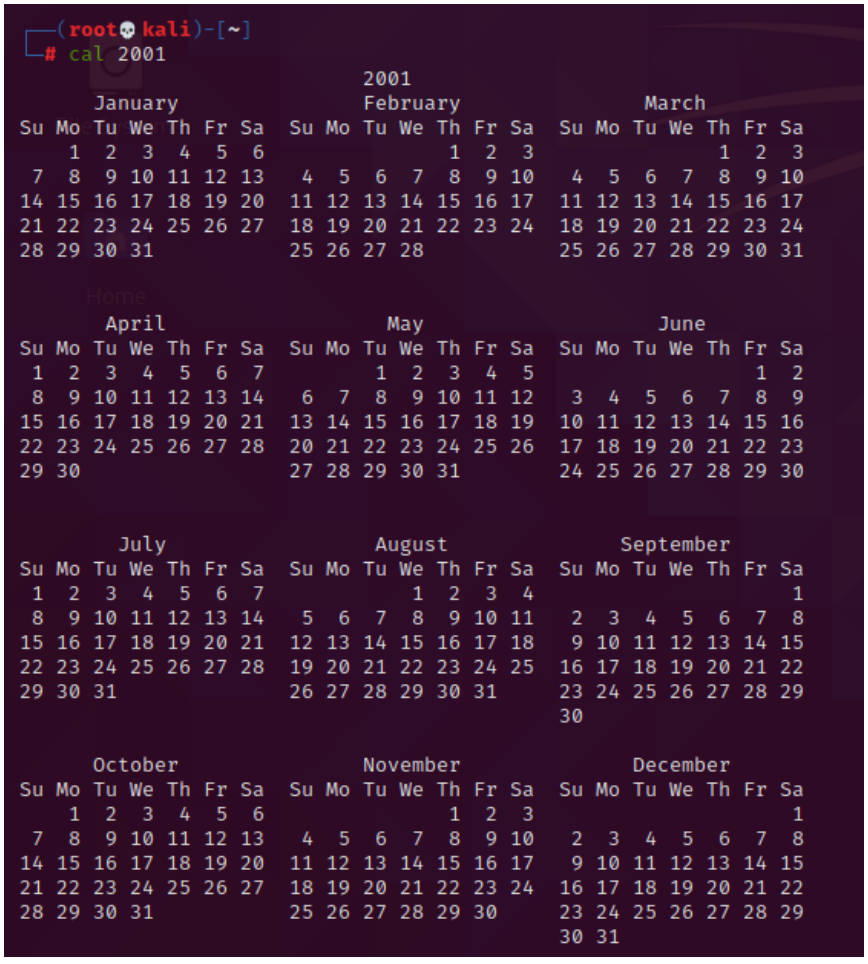
16. ls:

Description: It shows the list of files or folders.



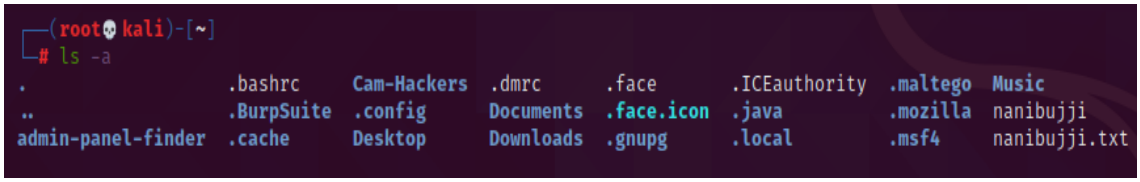
17. cal 'year we need':

Description: It displays the calendar of the year specified.



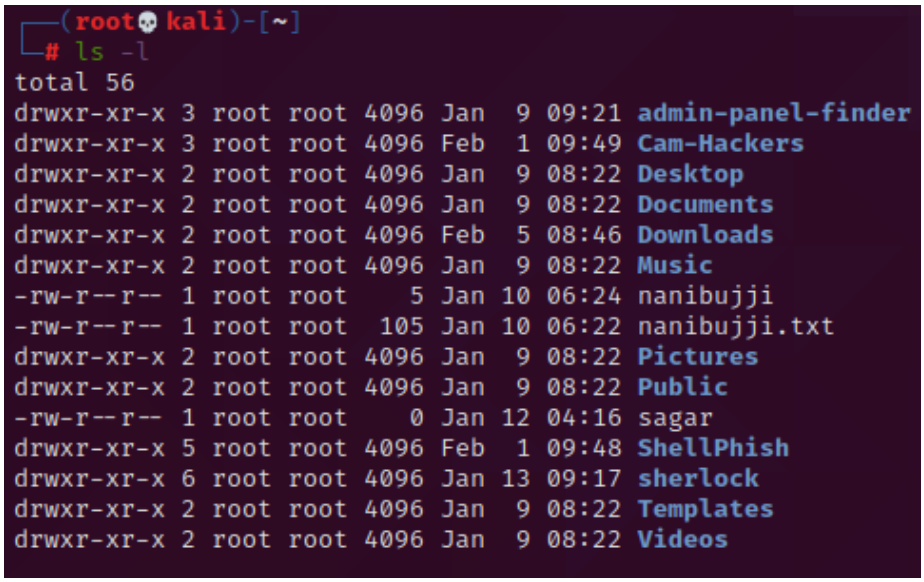
18. ls -a:

Description: To see the hidden folders.



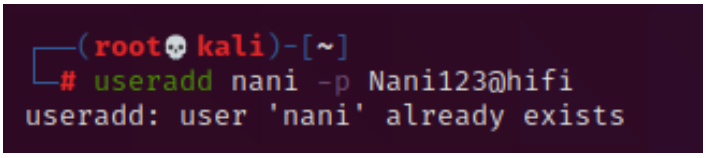
19. ls -l:

Description: It shows the data of the list of files and photos.



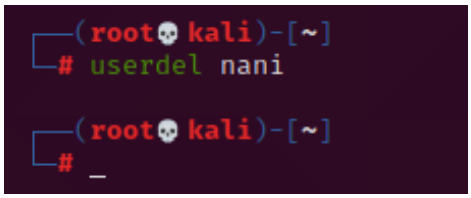
20. useradd -p password:

Description: Creating a password for the username.



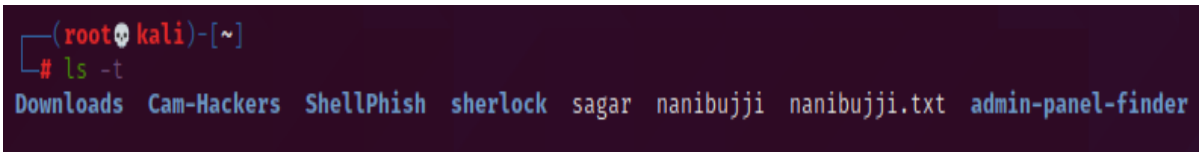
21. userdel name:

Description: To delete the username.



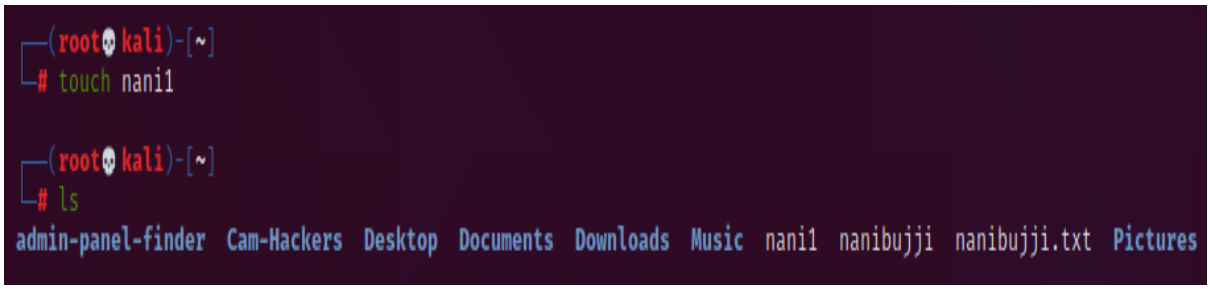
22. ls -t:

Description: Last modified files will be sorted.



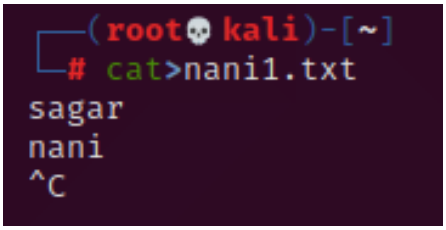
23. touch filename:

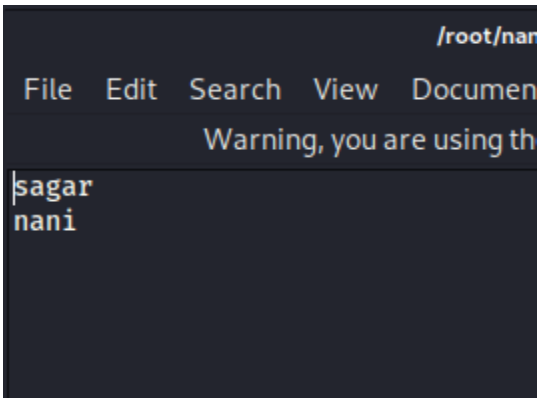
Description: To create a new file.



24. cat>filename.txt:

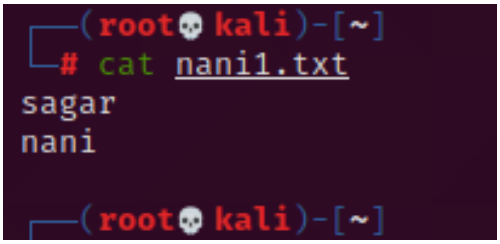
Description: Type then command with the filename needed and then press enter, then type the content to add to the file then press “ctrl C”, the content is sent to file





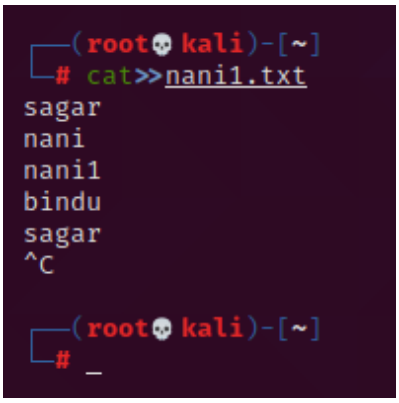
25. cat filename.txt:

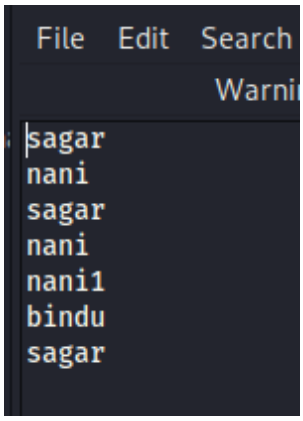
Description: saved content is shown.



26. cat>>filename:

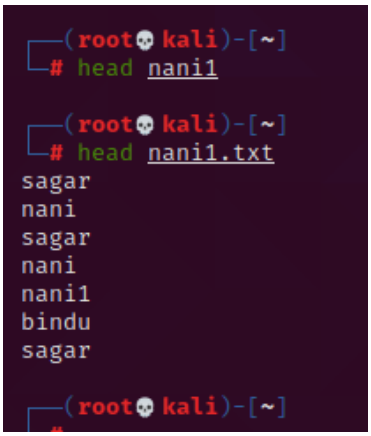
Description: The data we add will add to the already present data.





27. head filename:

Description: The first 10 lines are saved in a folder.

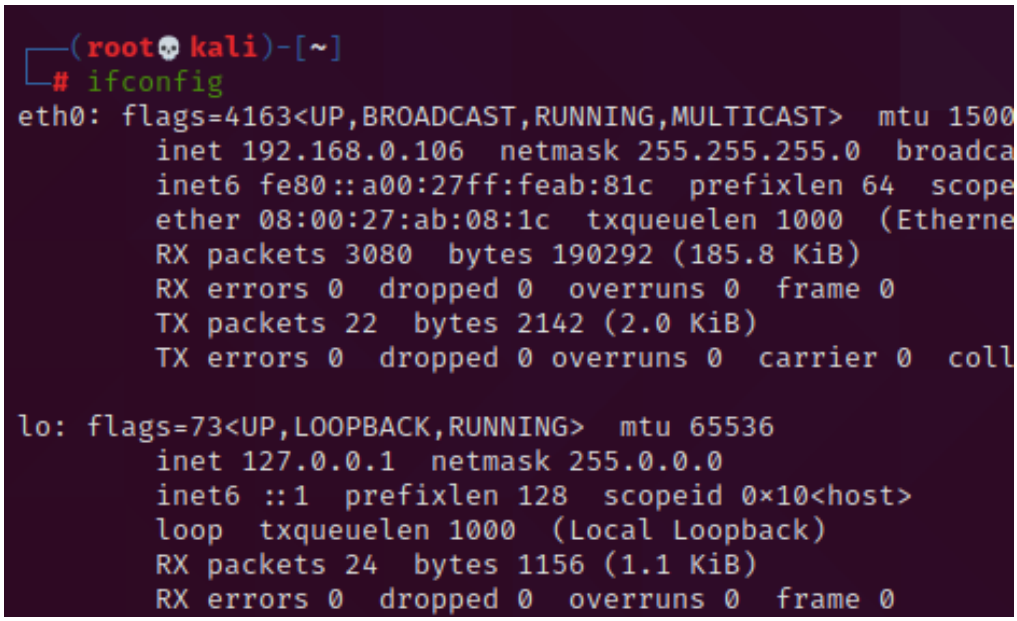


28. tail filename:

Description: last 10 lines saved in folder.

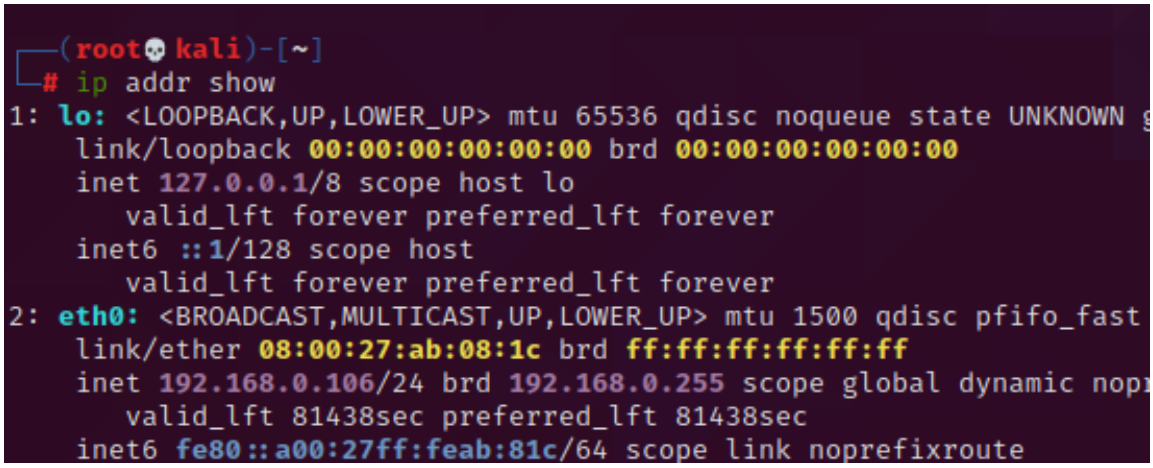
29. ifconfig:

Description: To see the configuration.



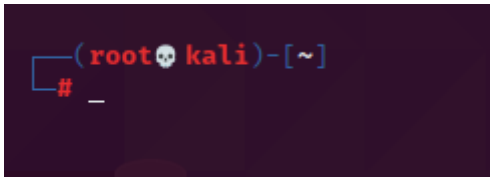
30. ip addr show:

Description: To show IP address.



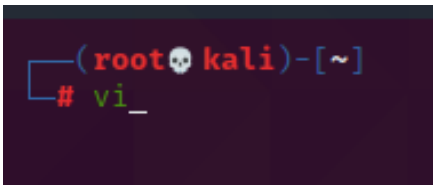
31. clear:

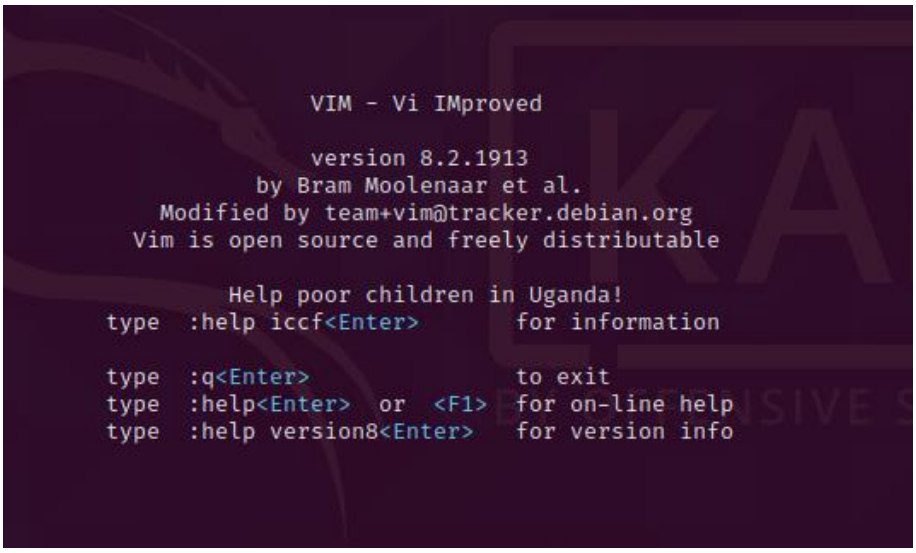
Description: to clear the screen.



32. vi:

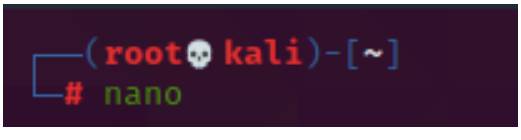
Description: opens the Vi editing command.

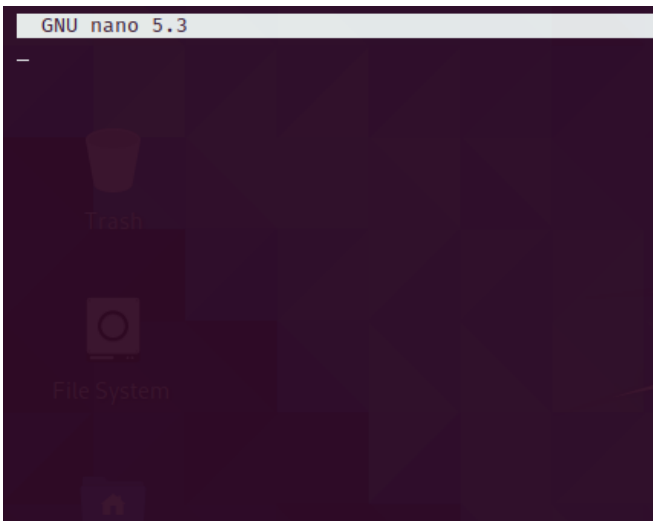




33. nano filename:

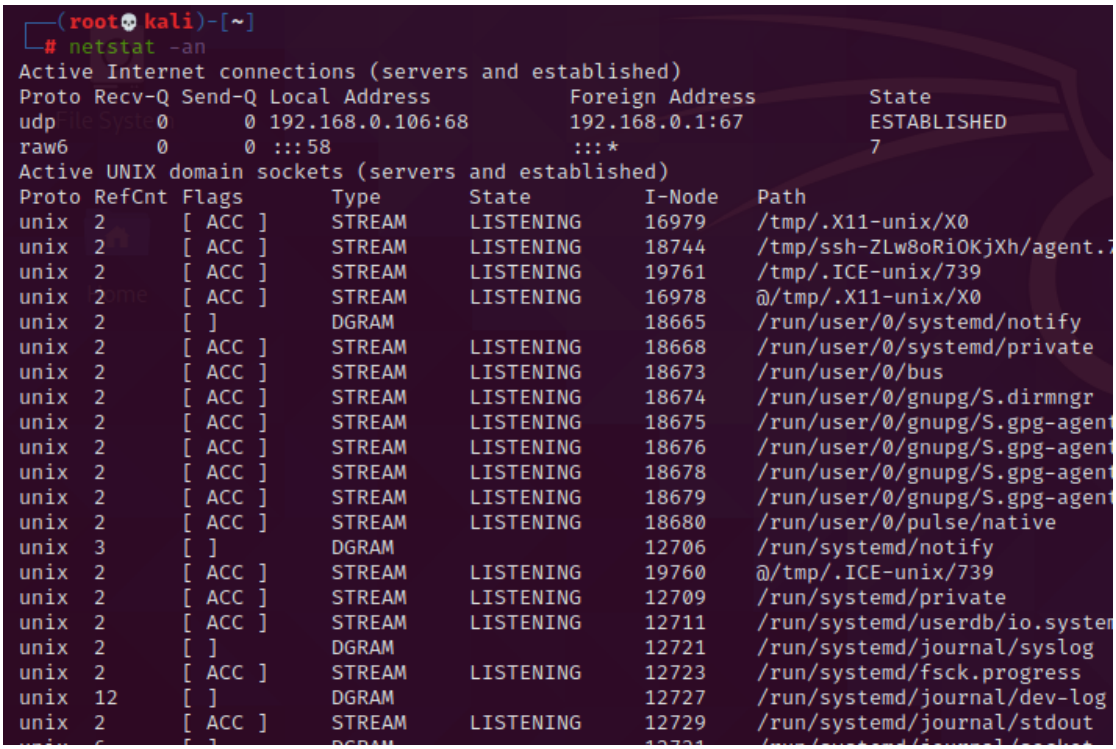
Description: open a file in nano editor.





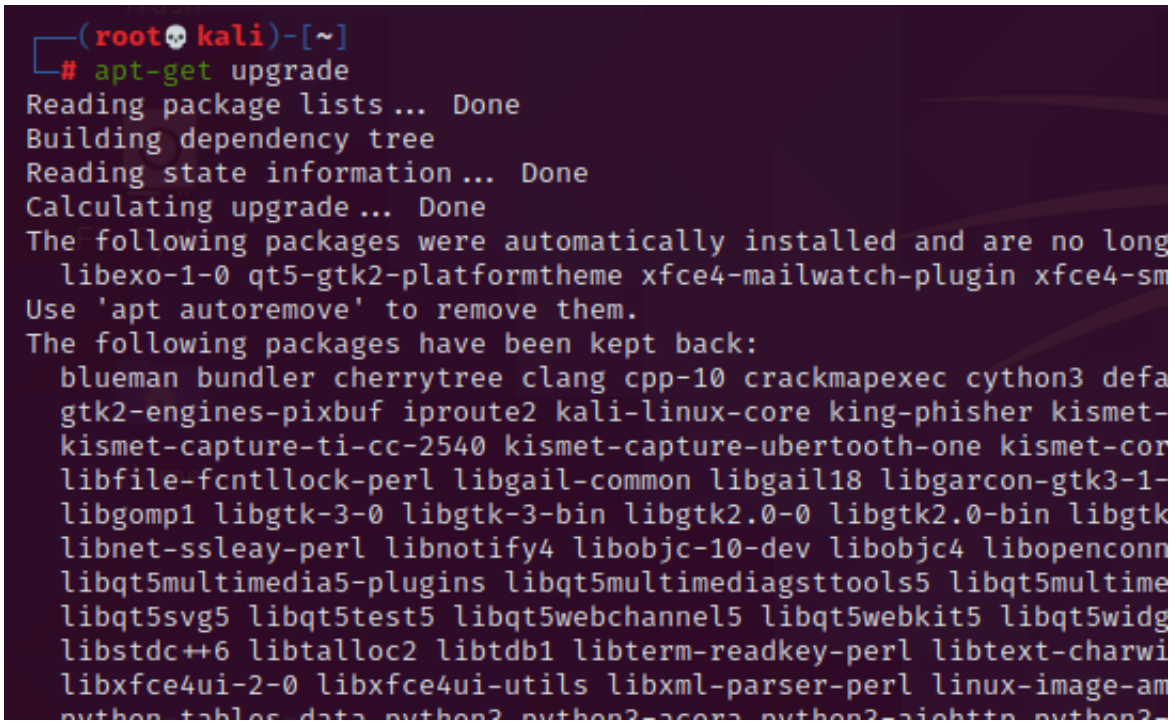
34. netstat _an:

Description: It displays all the network connections present to the system.



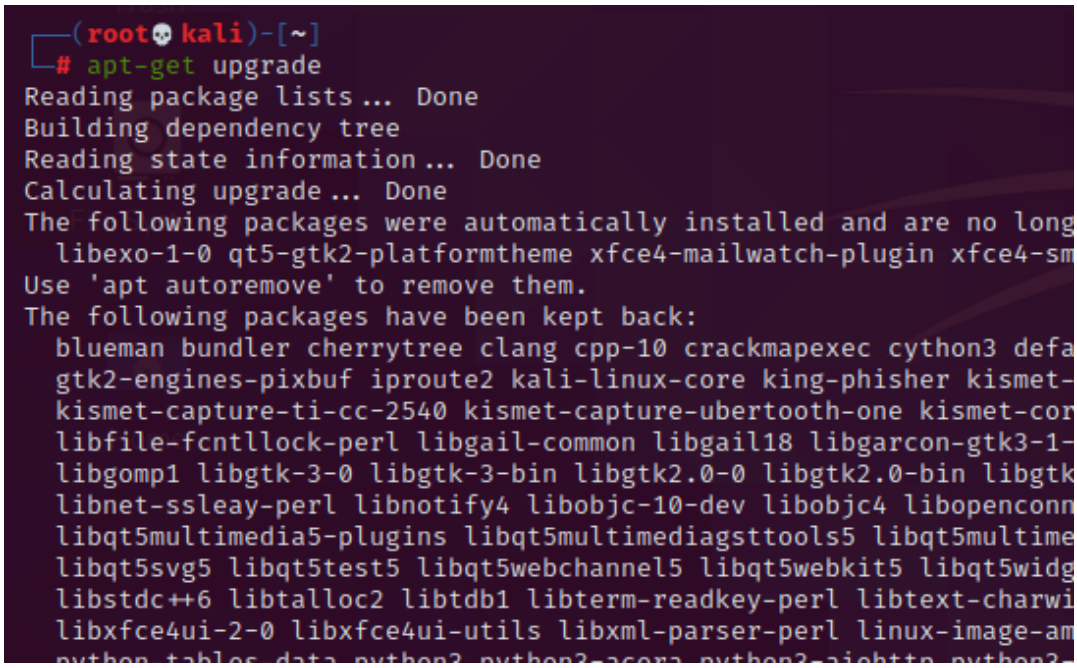
35. apt-get update:

Description: To update the Linux to the latest version.



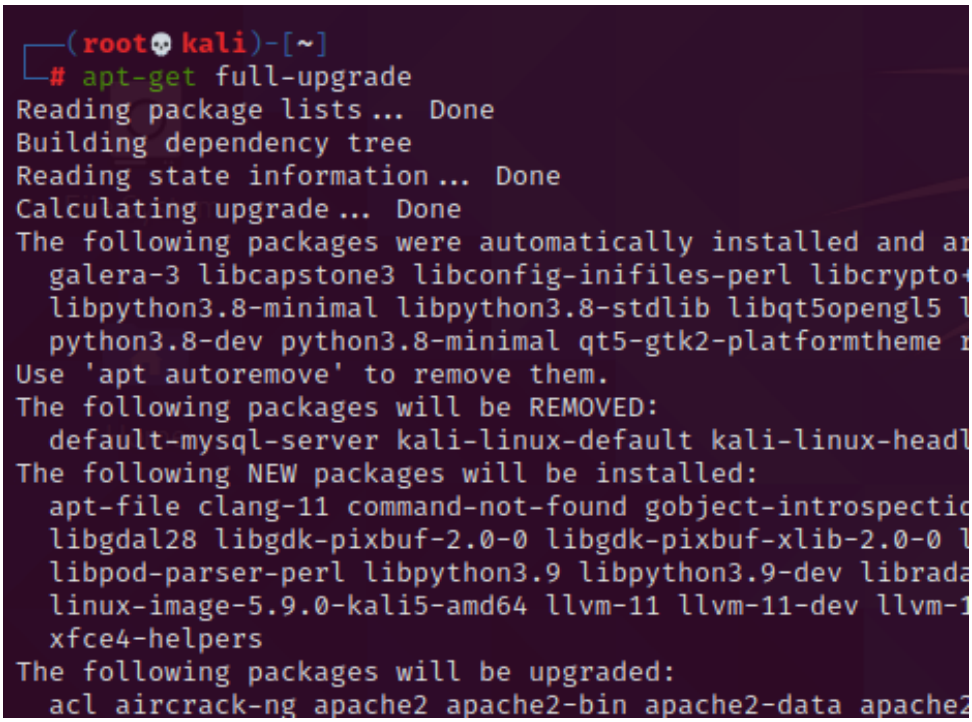
36. apt-get upgrade:

Description: To upgrade the Linux to its extent.



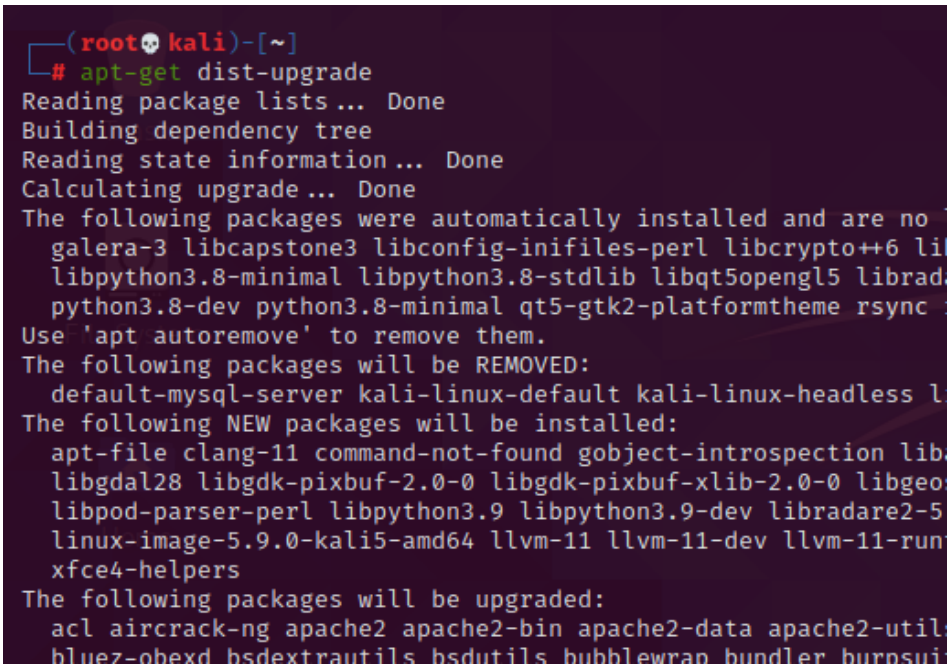
37. apt-get full-upgrade:

Description: To upgrade the code totally to its extreme new features and latest version.



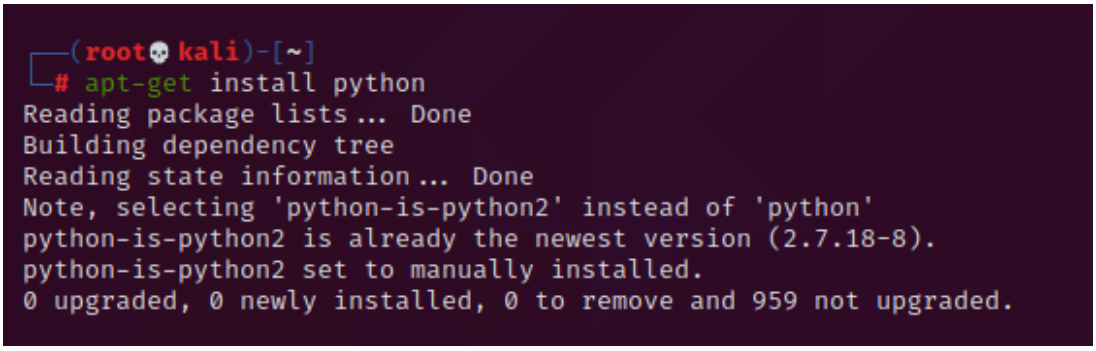
38. apt-get dist-upgrade:

Description: Distribution of upgrade as per the need.



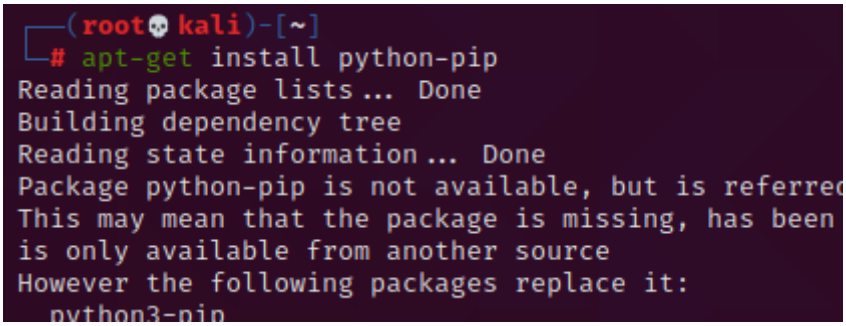
39. apt-get install python:

Description: To install the python.



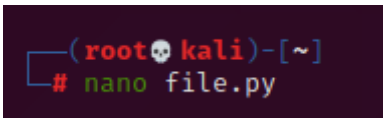
40. apt-get install python -pip:

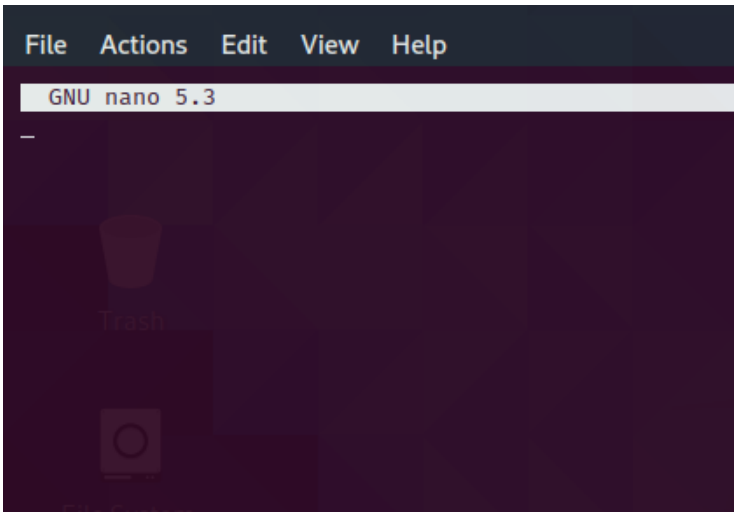
Description: To install the packages.



41. nano file.py:

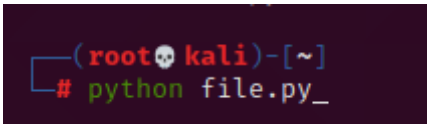
Description: creating a file in nano.





42. python file.py:

Description: To open or display the file.



43. chmod 777 file.py:

Description: used that file contain terms read, write, execute (777)

```
┌──(root💀kali)-[~]
└─# chmod 777 nani1.py

┌──(root💀kali)-[~]
└─# ls -l
total 68
drwxr-xr-x 3 root root 4096 Jan  9 09:21 admin-panel-finder
drwxr-xr-x 3 root root 4096 Feb  1 09:49 Cam-Hackers
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Desktop
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Documents
drwxr-xr-x 2 root root 4096 Feb  5 08:46 Downloads
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Music
-rw-r--r-- 1 root root    0 May 17 13:51 nani1
-rw------- 1 root root    2 May 17 14:24 nani12345.py.save
-rwxrwxrwx 1 root root   96 May 17 14:16 nani1.py
-rw-r--r-- 1 root root    5 Jan 10 06:24 nanibujji
-rw-r--r-- 1 root root  105 Jan 10 06:22 nanibujji.txt
-rw-r--r-- 1 root root   35 May 17 14:07 nanisagar.txt
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Pictures
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Public
-rw-r--r-- 1 root root    0 May 17 13:50 sagar
drwxr-xr-x 5 root root 4096 Feb  1 09:48 ShellPhish
drwxr-xr-x 6 root root 4096 Jan 13 09:17 sherlock
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Templates
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Videos
```

44. chmod +x file.py:

Description: To execute the file.

```
┌──(root💀kali)-[~]
└─# chmod +x nani1.py

┌──(root💀kali)-[~]
└─# ls -l
total 68
drwxr-xr-x 3 root root 4096 Jan  9 09:21 admin-panel-finder
drwxr-xr-x 3 root root 4096 Feb  1 09:49 Cam-Hackers
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Desktop
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Documents
drwxr-xr-x 2 root root 4096 Feb  5 08:46 Downloads
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Music
-rw-r--r-- 1 root root    0 May 17 13:51 nani1
-rw------- 1 root root    2 May 17 14:24 nani12345.py.save
-rwxrwxrwx 1 root root   96 May 17 14:16 nani1.py
-rw-r--r-- 1 root root    5 Jan 10 06:24 nanibujji
-rw-r--r-- 1 root root  105 Jan 10 06:22 nanibujji.txt
-rw-r--r-- 1 root root   35 May 17 14:07 nanisagar.txt
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Pictures
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Public
-rw-r--r-- 1 root root    0 May 17 13:50 sagar
drwxr-xr-x 5 root root 4096 Feb  1 09:48 ShellPhish
drwxr-xr-x 6 root root 4096 Jan 13 09:17 sherlock
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Templates
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Videos
```

45. chmod +r file.py:

Description: To read the file.

46. chmod +w file.py:

Description: To write the content in the file.

```
┌──(root💀kali)-[~]
└─# chmod +w nani1.py

┌──(root💀kali)-[~]
└─# ls -l
total 68
drwxr-xr-x 3 root root 4096 Jan  9 09:21 admin-panel-finder
drwxr-xr-x 3 root root 4096 Feb  1 09:49 Cam-Hackers
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Desktop
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Documents
drwxr-xr-x 2 root root 4096 Feb  5 08:46 Downloads
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Music
-rw-r--r-- 1 root root    0 May 17 13:51 nani1
-rw------- 1 root root    2 May 17 14:24 nani12345.py.save
-rw-rw-rw- 1 root root   96 May 17 14:16 nani1.py
-rw-r--r-- 1 root root    5 Jan 10 06:24 nanibujji
-rw-r--r-- 1 root root  105 Jan 10 06:22 nanibujji.txt
-rw-r--r-- 1 root root   35 May 17 14:07 nanisagar.txt
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Pictures
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Public
-rw-r--r-- 1 root root    0 May 17 13:50 sagar
drwxr-xr-x 5 root root 4096 Feb  1 09:48 ShellPhish
drwxr-xr-x 6 root root 4096 Jan 13 09:17 sherlock
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Templates
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Videos
```

47. history:

Description: To see all the history of the Linux terminal, that is all the commands types until then.

```
┌──(root💀kali)-[~]
└─# history
    1  userdel nani
    2  useradd nani
    3  userdel nani
    4  useradd nani -p Nani123@hifi
    5  login
    6  userdel nani
    7  useradd --help
    8  useradd nani
    9  useradd -p Nani123@hifi
   10  login root
   11  aafire
   12  apt-get install aafire
   13  nmap --script ftp-anon ftp.leo.org
   14  nmap --script ftp-anon ftp.esat.net
   15  nmap --script ftp-anon ftp.tu-chemnitz.de
   16  nmap --script ftp-anon ftp.iamas.ac.jp
   17  ifconfig
   18  netdiscover
   19  nmap 192.168.43.207
   20  nmap -sV 192.168.43.207
   21  nmap --A 192.168.43.207
   22  nmap -A 192.168.43.207
   23  dirb http://192.168.43.207
   24  msfconsole
```

48. chmod 555 file.py:

Description: It helps to change the functional permissions such as read and execute.

```
┌──(root💀kali)-[~]
└─# chmod 555 nani1.py

┌──(root💀kali)-[~]
└─# ls -l
total 72
drwxr-xr-x 3 root root 4096 Jan  9 09:21 admin-panel-finder
-rw-r--r-- 1 root root   24 May 18 10:36 bindusagar.jar
drwxr-xr-x 3 root root 4096 Feb  1 09:49 Cam-Hackers
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Desktop
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Documents
drwxr-xr-x 2 root root 4096 Feb  5 08:46 Downloads
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Music
-rw-r--r-- 1 root root    0 May 17 13:51 nani1
-rw------- 1 root root    2 May 17 14:24 nani12345.py.save
-r-xr-xr-x 1 root root   96 May 17 14:16 nani1.py
-rw-r--r-- 1 root root    5 Jan 10 06:24 nanibujji
-rw-r--r-- 1 root root  105 Jan 10 06:22 nanibujji.txt
-rw-r--r-- 1 root root   35 May 17 14:07 nanisagar.txt
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Pictures
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Public
-rw-r--r-- 1 root root    0 May 17 13:50 sagar
drwxr-xr-x 5 root root 4096 Feb  1 09:48 ShellPhish
drwxr-xr-x 6 root root 4096 Jan 13 09:17 sherlock
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Templates
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Videos
```

49. unzip file name:

Description: zip file will be unzipped.

```
┌──(root💀kali)-[~]
└─# unzip nanibujji
Archive:  nanibujji
  End-of-central-directory signature not found.  Either this file is not
  a zipfile, or it constitutes one disk of a multi-part archive.  In the
  latter case the central directory and zipfile comment will be found on
  the last disk(s) of this archive.
unzip:  cannot find zipfile directory in one of nanibujji or
        nanibujji.zip, and cannot find nanibujji.ZIP, period.
```

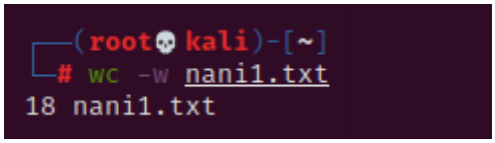
50. gunzip file name:

Description: To decompress the Gzip files (they are given with gz or z extension).

```
┌──(root💀kali)-[~]
└─# gunzip nanibujji
gzip: nanibujji: unknown suffix -- ignored
```

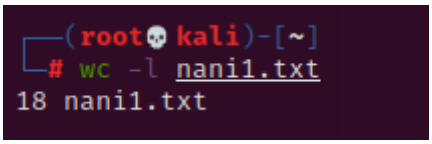
51. wc -w file.txt:

Description: To count number of words in file.



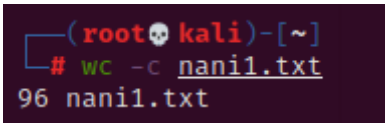
52. wc -l file.txt:

Description: To count the number of lines in file.



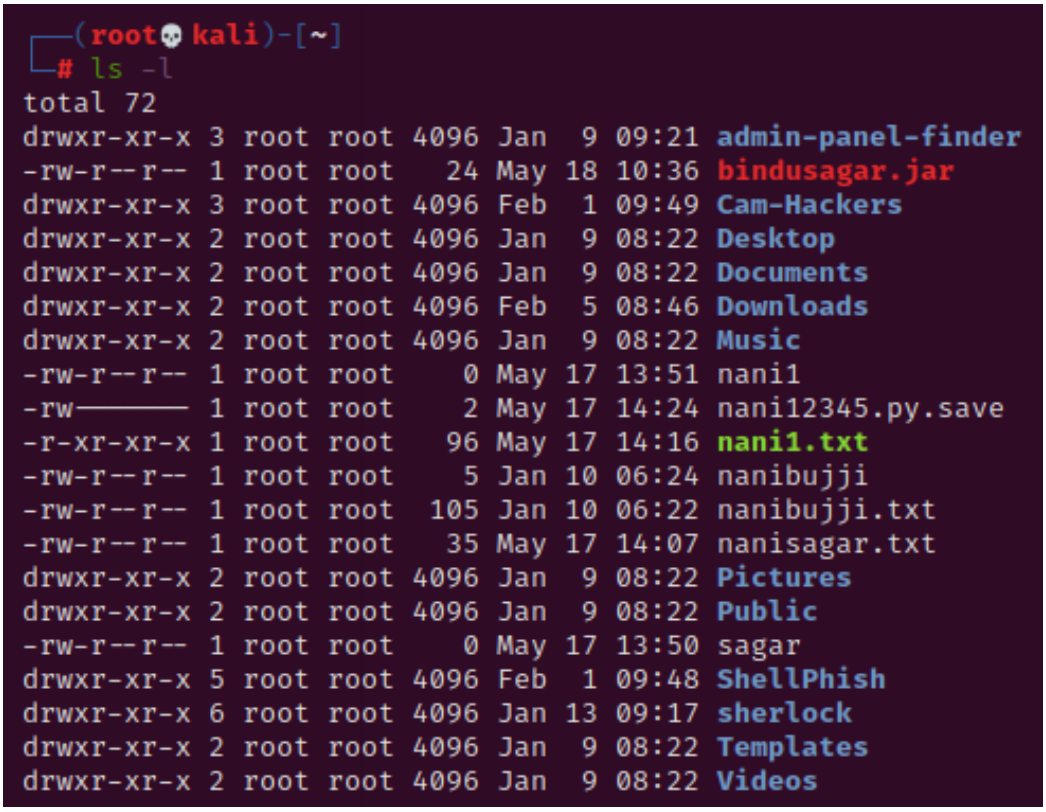
53. wc -c file.txt:

Description: To count the number of characters in the file.



54. ls-l:

Description: displays the present working directory.



55. vim:

Description: open the vim editing command.

```
┌──(root💀kali)-[~]
└─# vim
```

```
                VIM - Vi IMproved

                version 8.2.1913
           by Bram Moolenaar et al.
     Modified by team+vim@tracker.debian.org
   Vim is open source and freely distributable

          Help poor children in Uganda!
 type  :help iccf<Enter>       for information

 type  :q<Enter>               to exit
 type  :help<Enter>  or  <F1>  for on-line help
 type  :help version8<Enter>   for version info
```

56. dd:

Description: It helps in convert and copy files.

```
┌──(root💀kali)-[~]
└─# dd
nani1
nanibujji
^C0+2 records in
0+0 records out
0 bytes copied, 11.3034 s, 0.0 kB/s
```

57. netstat -g:

Description: It helps in displaying multicast membership information for both IPv4 and IPv6.

```
┌──(root💀kali)-[~]
└─# netstat -g
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      all-systems.mcast.net
eth0            1      all-systems.mcast.net
lo              1      ip6-allnodes
lo              1      ff01::1
eth0            1      ff02::1:ffab:81c
eth0            1      ip6-allnodes
eth0            1      ff01::1
```

58. netstat -r:

Description: It helps in displaying kernel IP routing table.

```
┌──(root💀kali)-[~]
└─# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.0.1     0.0.0.0         UG        0 0          0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

59. q:

Description: It helps in displaying the network interface packet transactions including both transferring and receiving packets.

```
┌──(root💀kali)-[~]
└─# netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500     5524      0      0 0           56      0      0      0 BMRU
lo       65536       90      0      0 0           90      0      0      0 LRU
```

60. man any command:

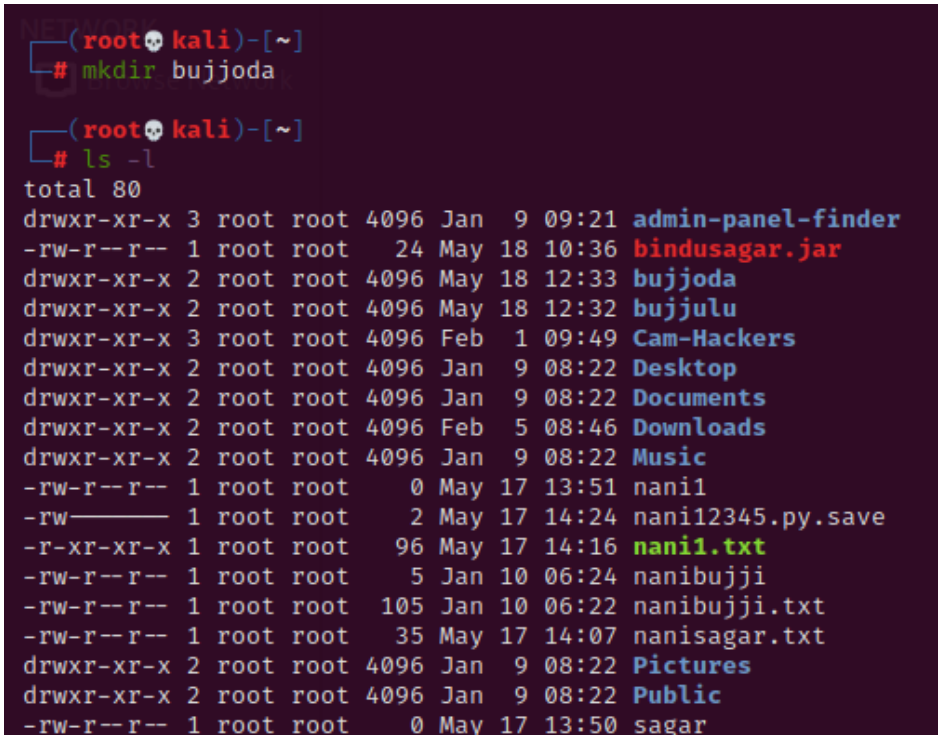
Description: It displays complete details of that command.

```
┌──(root💀kali)-[~]
└─# man ls
```

```
LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List information about the FILEs (the current directory by default).  Sort entries alphabetically if

       Mandatory arguments to long options are mandatory for short options too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
              do not list implied . and ..

       --author
              with -l, print the author of each file

       -b, --escape
              print C-style escapes for nongraphic characters

       --block-size=SIZE
              with -l, scale sizes by SIZE when printing them; e.g., '--block-size=M'; see SIZE format belo

       -B, --ignore-backups
              do not list implied entries ending with ~

       -c     with -lt: sort by, and show, ctime (time of last modification of file status information); wi

       -C     list entries by columns
```

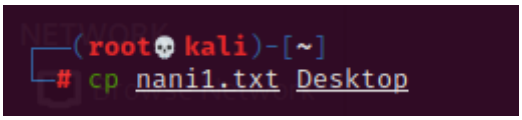
61. mkdir:

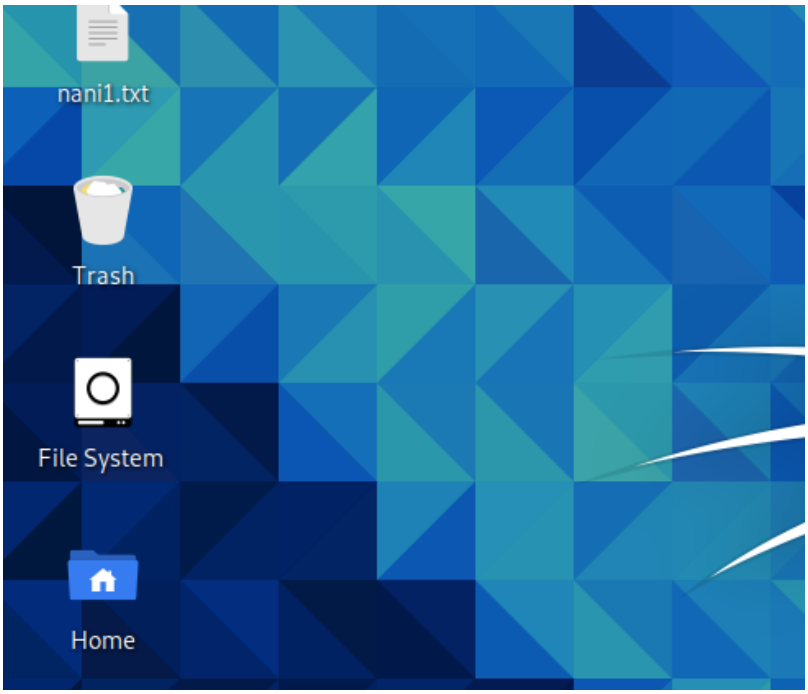
Description: To create a new file in the specified location.



62. cp file.txt:

Description: To copy the file to specified address.

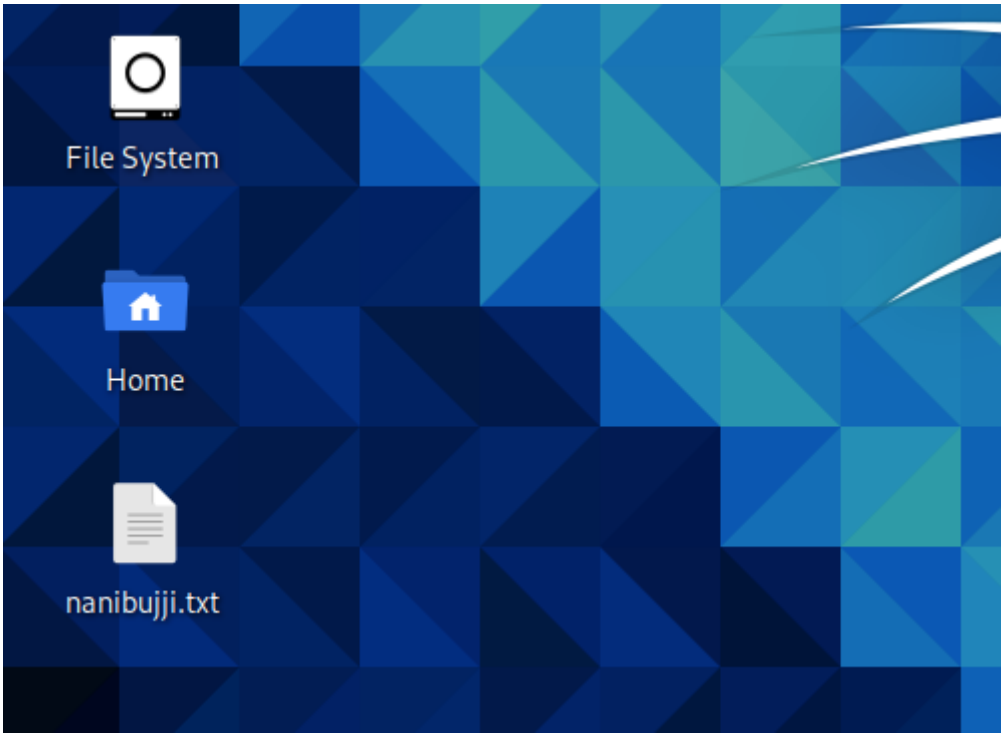




63. mv:

Description: To move a file from one location to the other location.

```
┌──(root💀kali)-[~]
└─# mv nanibujji.txt Desktop
```



64. rm:

Description: To remove or delete the files.

```
┌──(root💀kali)-[~]
└─# ls
admin-panel-finder  bujjoda  busa         Desktop    Downloads  nani1             nani1.txt  nanisaga
bindusagar.jar      bujjulu  Cam-Hackers  Documents  Music      nani12345.py.save  nanibujji  Pictures

┌──(root💀kali)-[~]
└─# rm busa

┌──(root💀kali)-[~]
└─# ls
admin-panel-finder  bindusagar.jar  bujjoda  bujjulu  Cam-Hackers  Desktop  Documents  Downloads  Musi
```

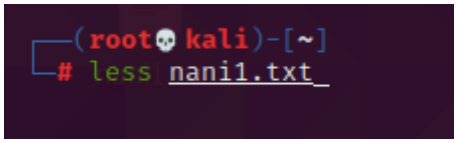
65. users:

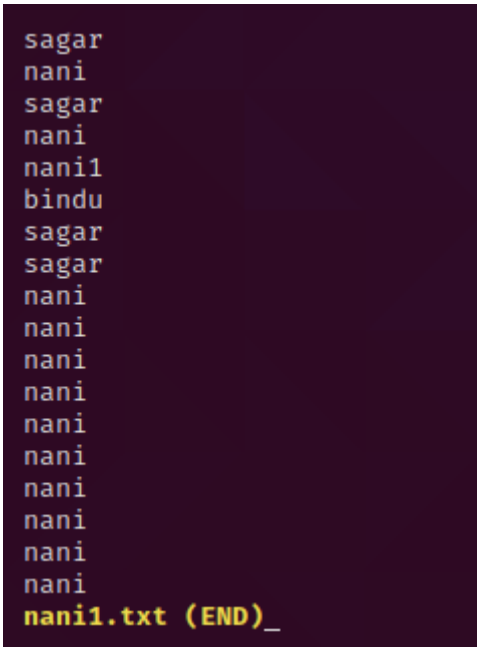
Description: It displays the user's name.

```
┌──(root💀kali)-[~]
└─# users
root
```

66. less:

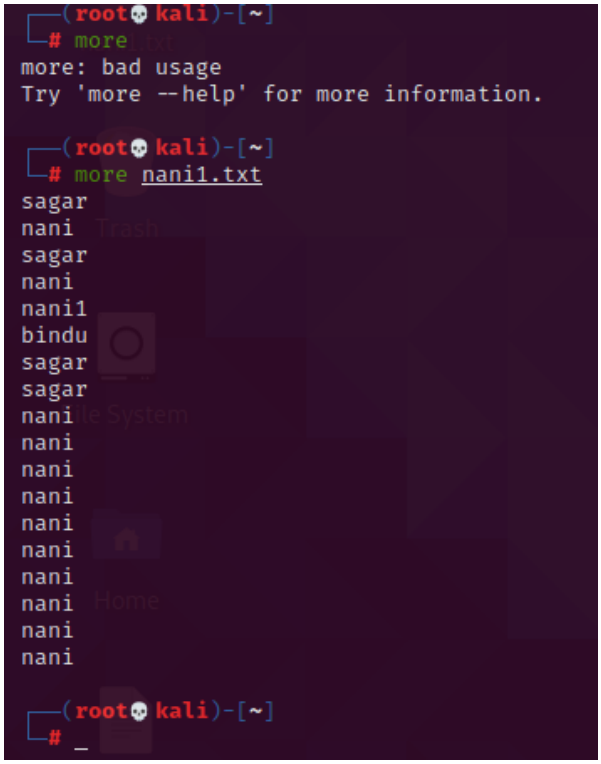
Description: It is used to view the files instead of opening the file.





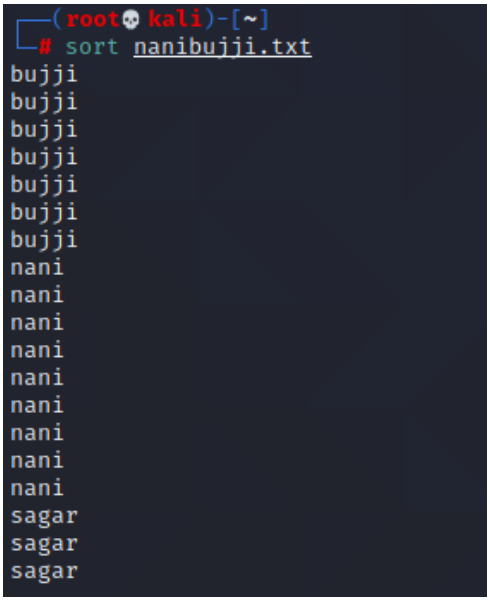
67. more:

Description: It allows you to display the output in the terminal one page at a time.



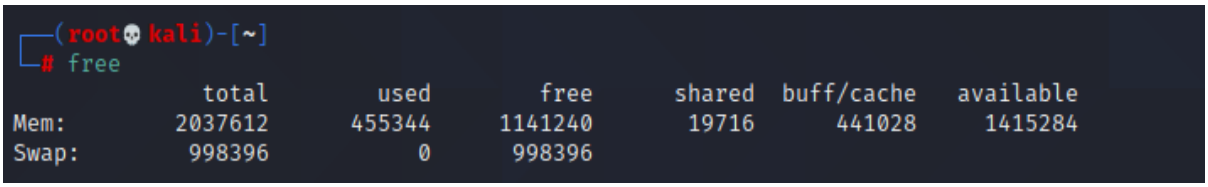
68. sort file.txt:

Description: It sorts the contents of a text file line by line.



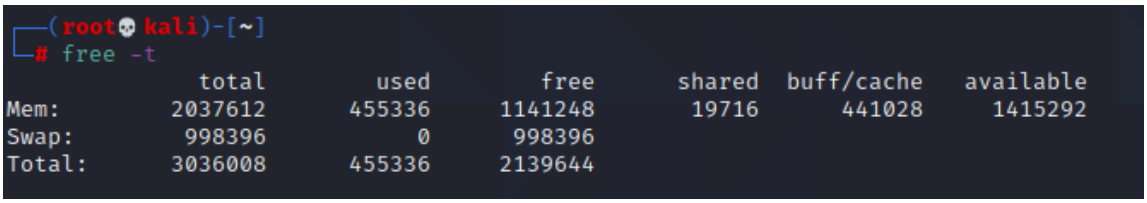
69. free:

Description: It gives the valuable information on available RAM in Linux machine.



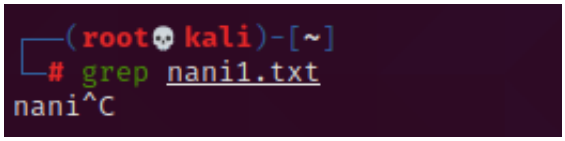
70. free -t:

Description: It will list the total line at the end.



71. grep:

Description: It helps in searching plain text data sheet from lines that match a normal expression.



72. chage:

Description: It is change age command and it can be used to change the expiry information of the user's password.

```
┌──(root💀 kali)-[~]
└─# chage root
Changing the aging information for root
Enter the new value, or press ENTER for the default

        Minimum Password Age [0]: _
```

73. df:

Description: To get all the information of your file system.

```
┌──(root💀 kali)-[~]
└─# df
Filesystem     1K-blocks    Used Available Use% Mounted on
udev              985152       0    985152   0% /dev
tmpfs             203764     924    202840   1% /run
/dev/sda1       81058256 9399684  67497960  13% /
tmpfs            1018804       0   1018804   0% /dev/shm
tmpfs               5120       0      5120   0% /run/lock
tmpfs               4096       0      4096   0% /sys/fs/cgroup
tmpfs             203760      52    203708   1% /run/user/0
```

74. df -h:

Description: To display all the file system information that is in human readable format.

```
┌──(root💀 kali)-[~]
└─# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            963M     0  963M   0% /dev
tmpfs           199M  924K  199M   1% /run
/dev/sda1        78G  9.0G   65G  13% /
tmpfs           995M     0  995M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           4.0M     0  4.0M   0% /sys/fs/cgroup
tmpfs           199M   52K  199M   1% /run/user/0
```

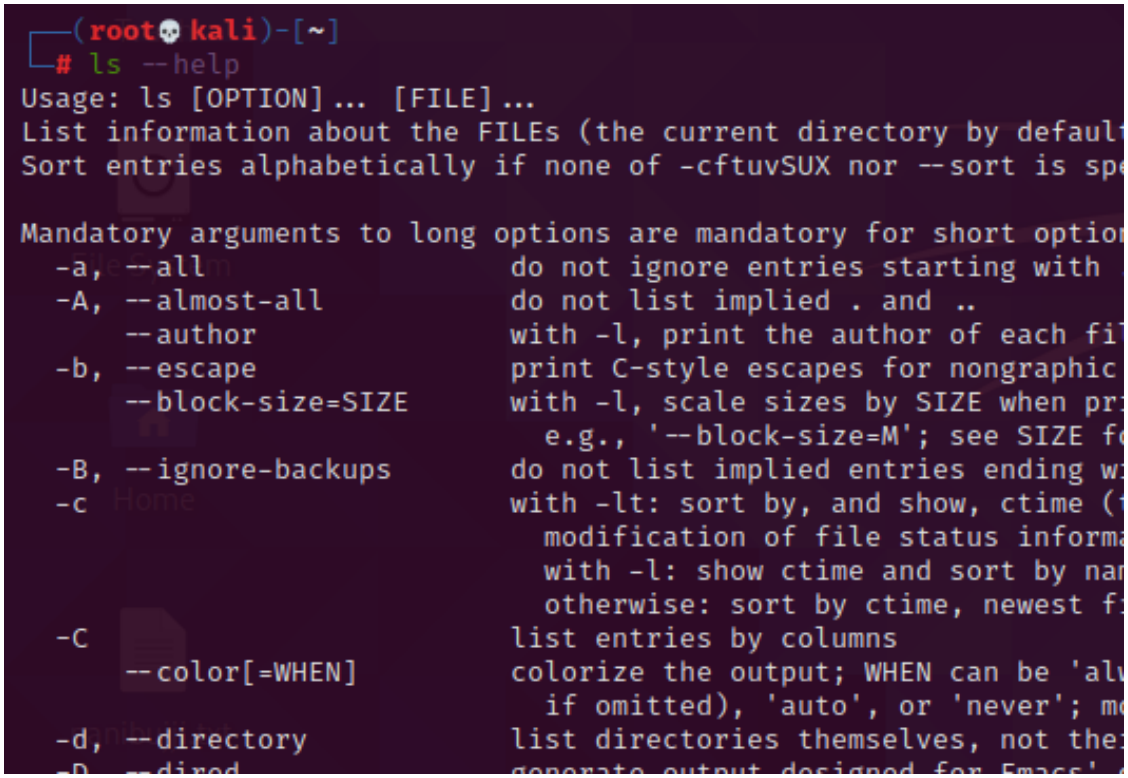
75. exit:

Description: It is used to close the terminal shell window directly from the command window.

```
sagar
sagar^C

┌──(root💀 kali)-[~]
└─# exit
```

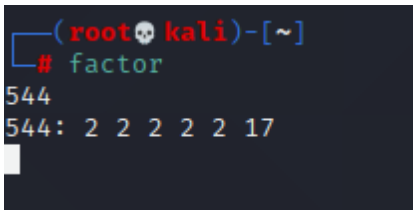
76. any command --help:

Description: It will list all built-in commands you can use in shell.



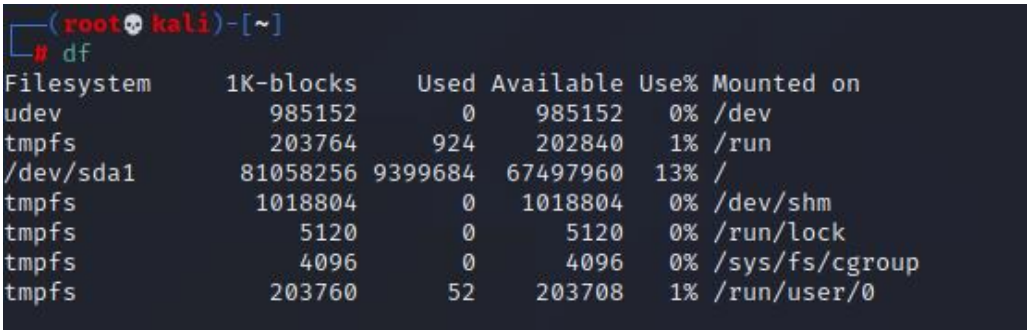
77. factor:

Description: It is a mathematical command for Linux terminal which will give you all the possible factors of the decimal number entered in the shell.



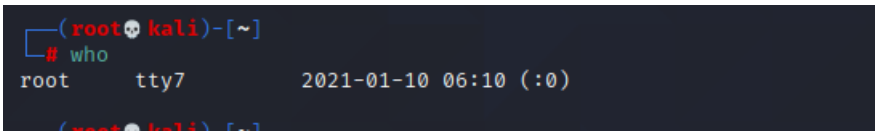
78. whatis <*command*>:

Description: To know the use of a particular command.



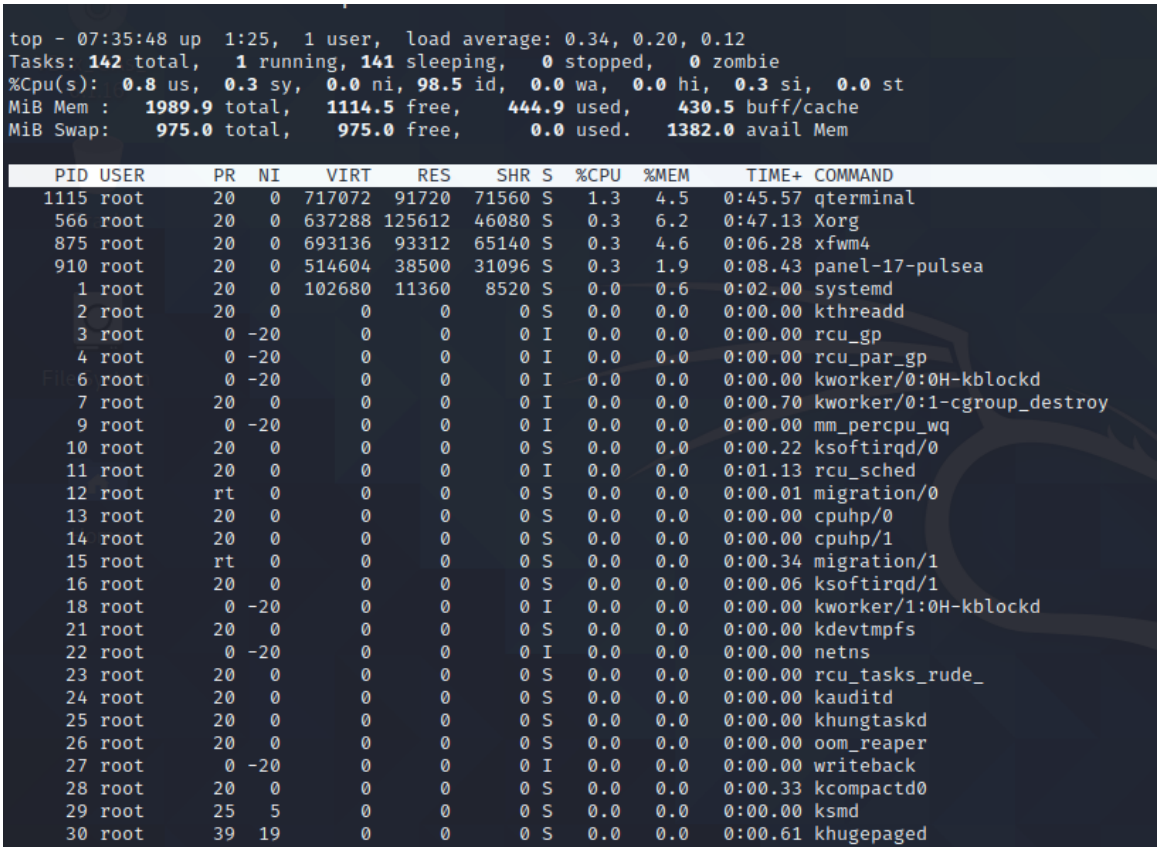
79. who:

Description: The one is for system administrators who handle and manage various users on Linux system. It shows all the users who are currently logged into the Linux system.



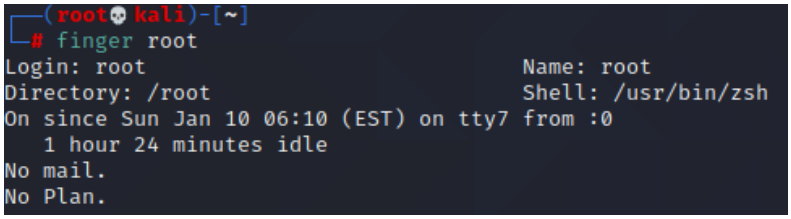
80. top:

Description: It is used to monitor all the ongoing processes on the Linux system with the username, priority level, unique process id and shared memory by each task.



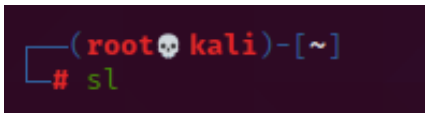
81. finger user:

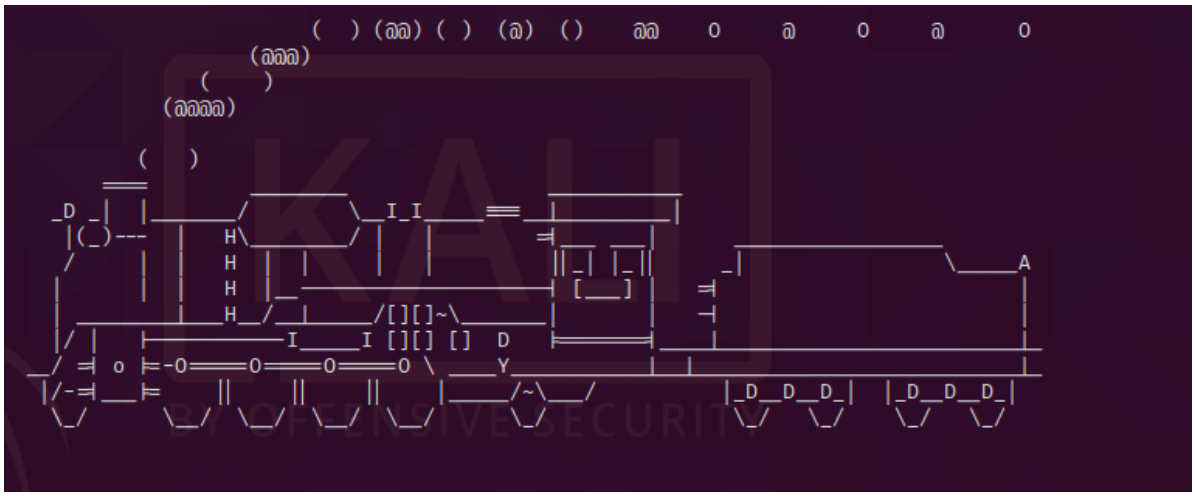
Description: It displays all the pillars about any user on the system.



82. sl:

Description: This is a fun command, when executed a steam engine passes through Terminal window. (sudo apt install sl)



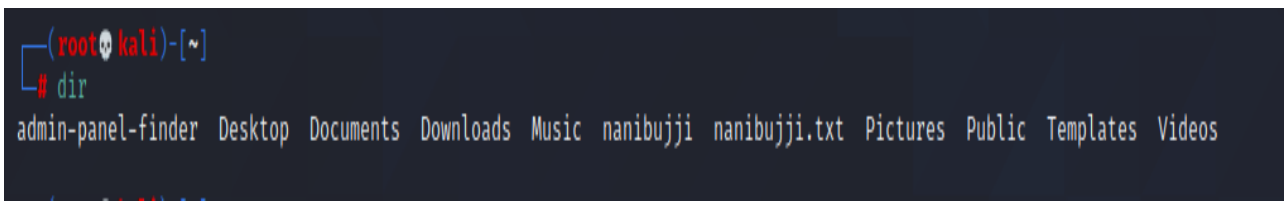


83. banner <*text*>:

Description: It is also a fun command for Linux Terminal when executed with banner and text. The text will be displayed in big banner format.

84. dir:

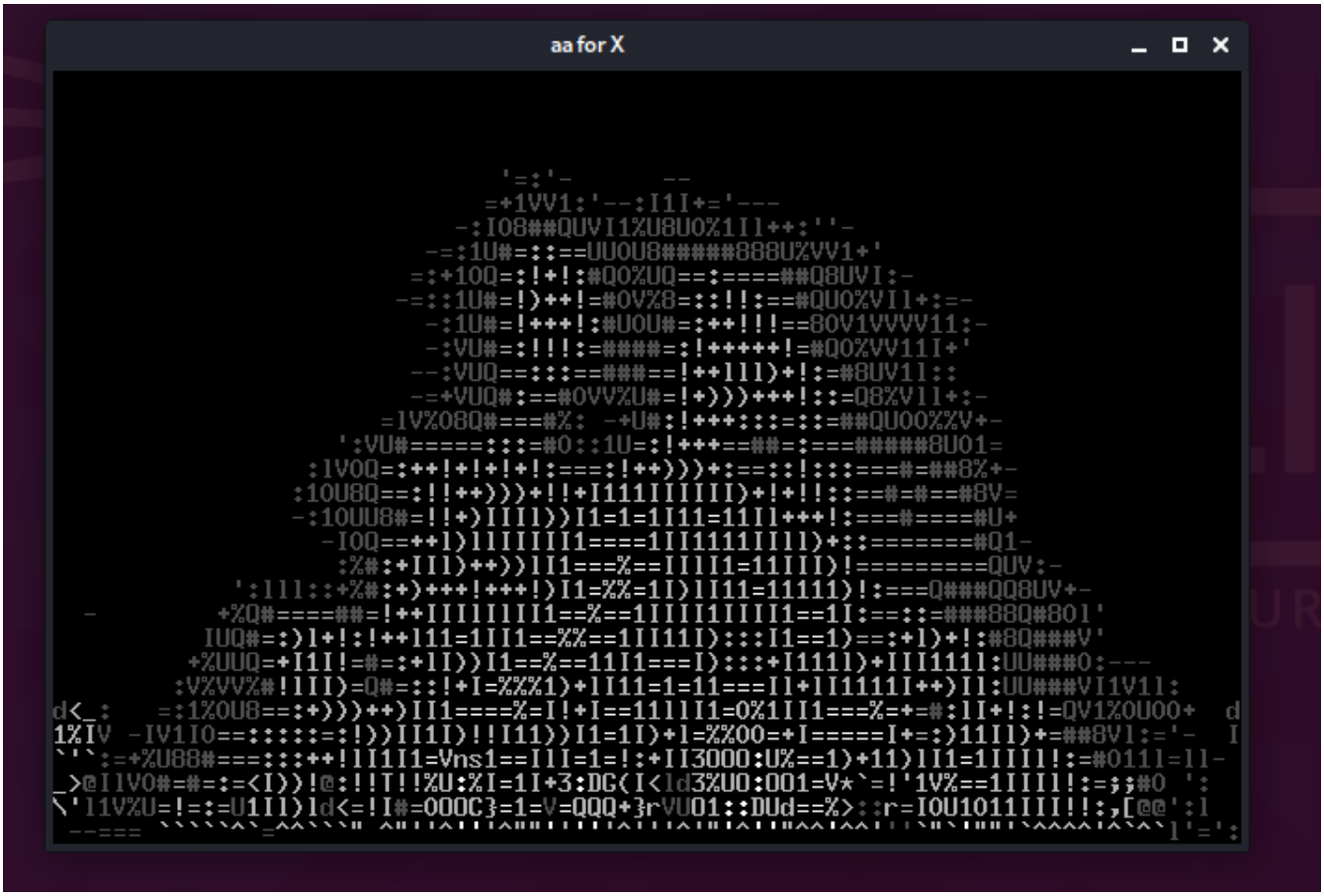
Description: It is used to view the list of all directories and folders present in current working directory.



85. aafire:

Description: It is a fun command it displays like as it puts the terminal in fire.

```
┌──(root💀 kali)-[~]
└─# aafire_
```



86. echo:

Description: It is used to print any text to type through with the command.

```
┌──(root💀 kali)-[~]
└─# echo nani
nani
```

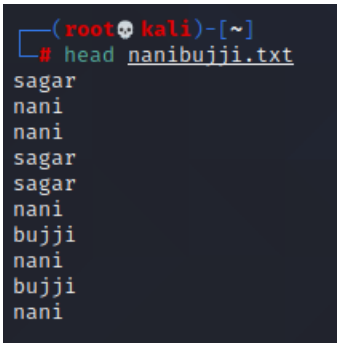
87. groups user:

Description: To know in which a particular user is part of.

```
┌──(root💀 kali)-[~]
└─# groups root
oot : root kaboxer

┌──(root💀 kali)-[~]
```

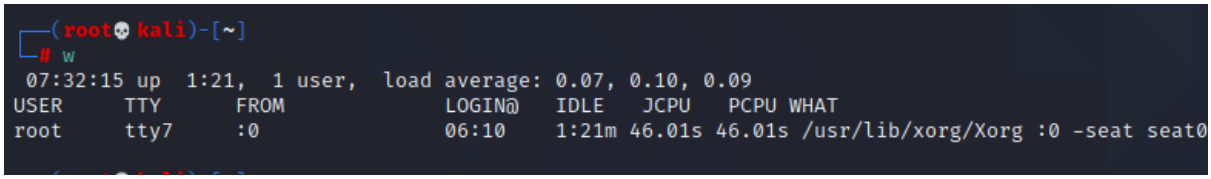
88. head filename:

Description: This command will list the first 10 lines of the file.



89. w:

Description: It is used to view the currently logged in users.



90. login:

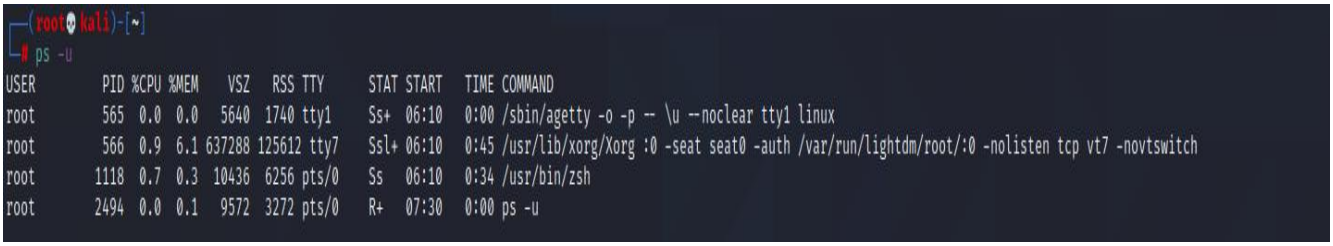
Description: It is used to switch user from one to another.

91. lscpu:

Description: It displays all the CPU information architecture information.

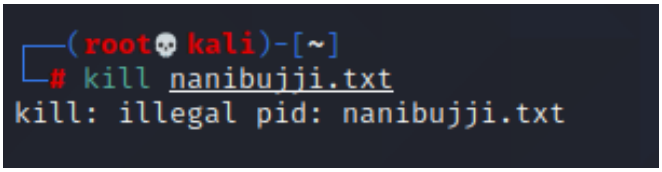
92. ps -u:

Description: It displays all the processes running in the system.



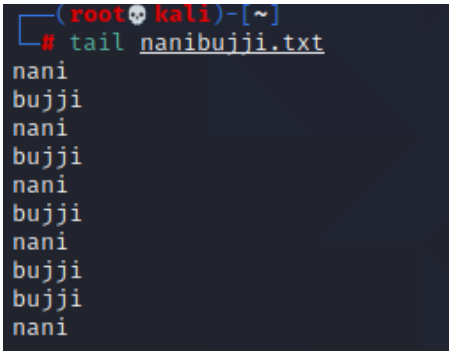
93. kill:

Description: It is used to kill the currently running process in the system.



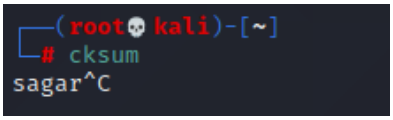
94. tail:

Description: It executes the last 10 lines of the file mentioned with this command.



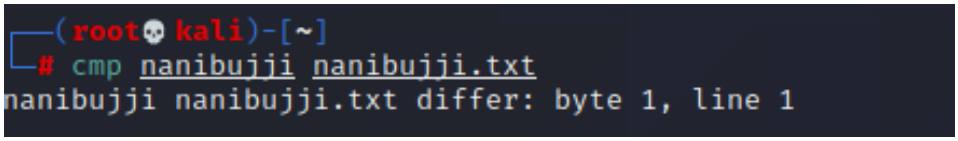
95. cksum:

Description: It is used to generate the checksum value for the file or stream of data thrown with command.



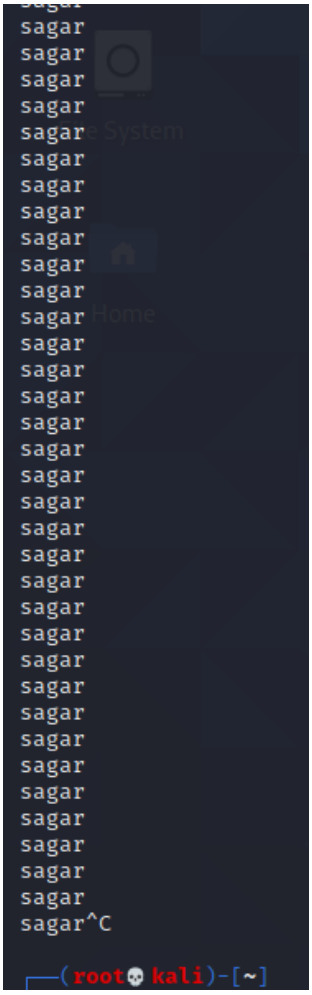
96. cmp:

Description: It is used to for byte by byte comparing of the files.



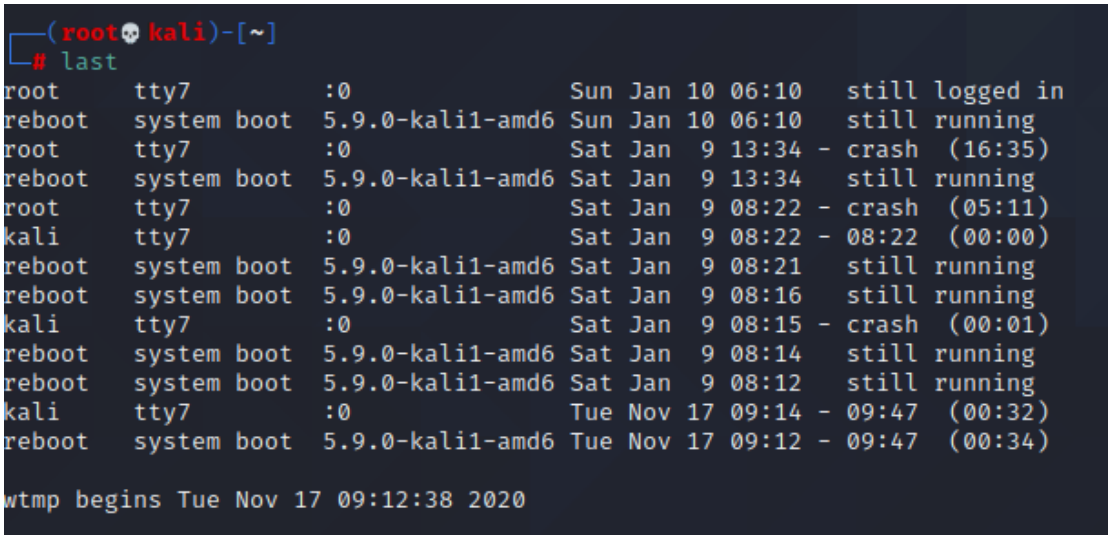
97. yes <text>:

Description: It executes the text continuously until you stop it with ctrl+ c



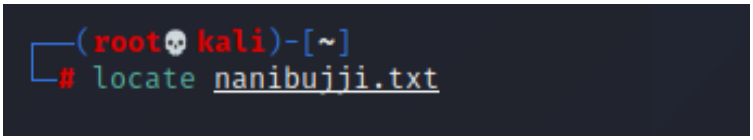
98. last:

Description: It displays the last logged in users into the system.



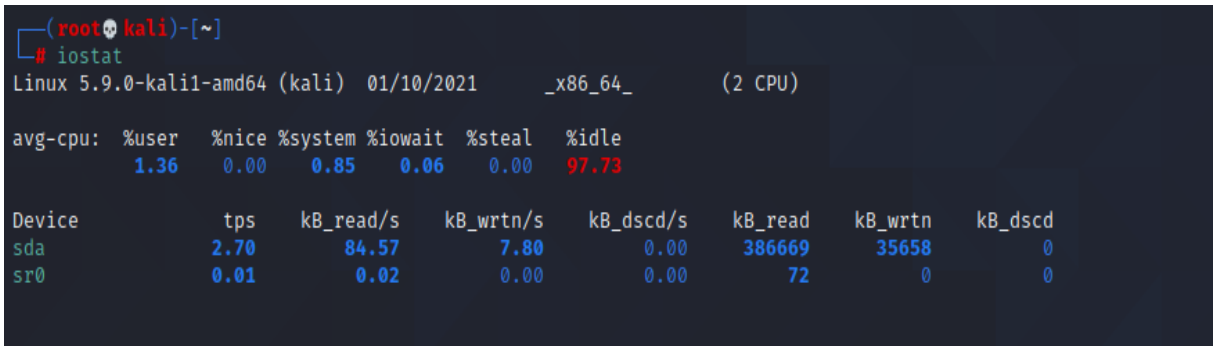
99. locate:

Description: It can be used to locate any type of file



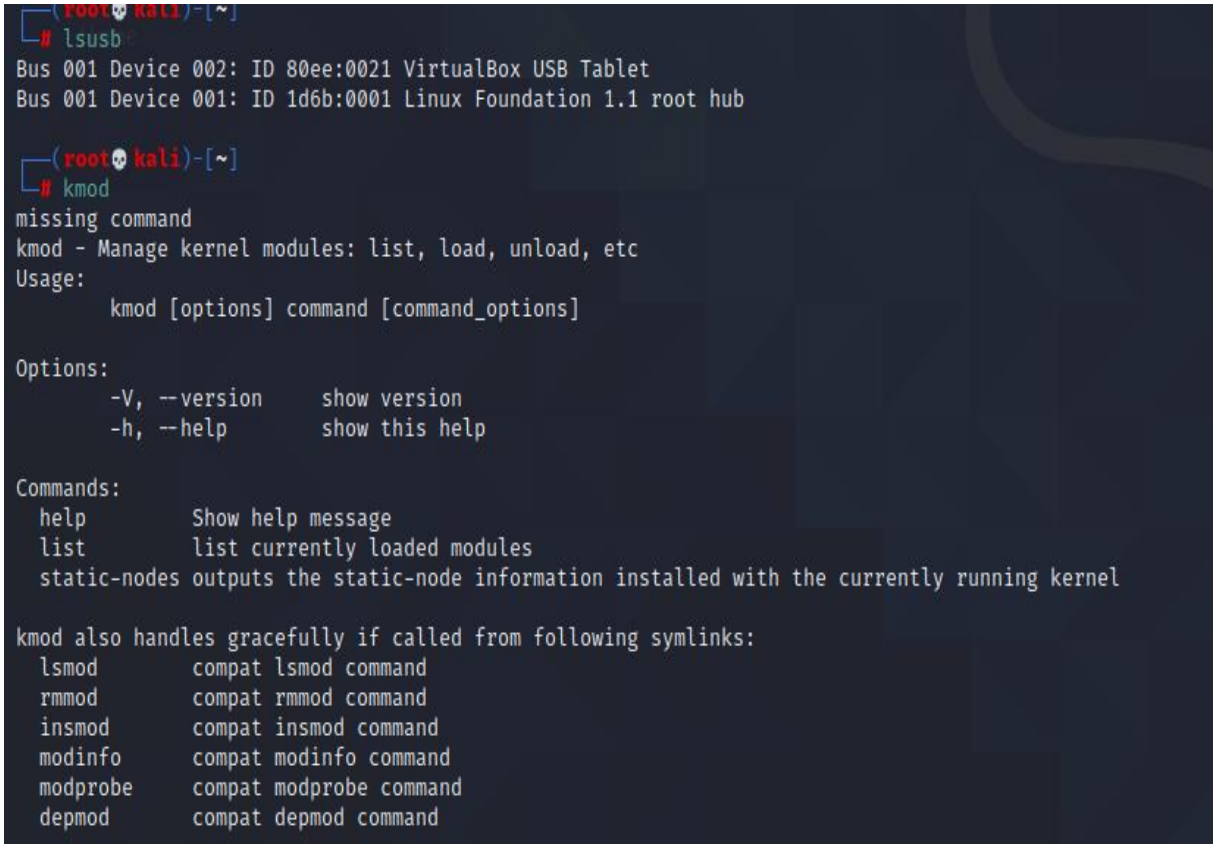
100. iostat:

Description: It displays all the stats of the CPU as well as input output devices in terminal window shell.



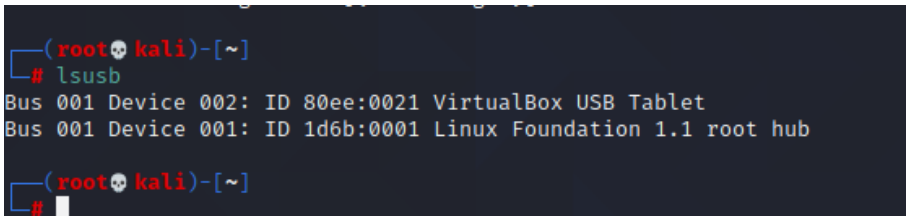
101. kmod:

Description: It displays all the currently loaded modules on the system.



102. lsusb:

Description: It shows information about all USB buses connected to the hardware and eternal USB devices connected.

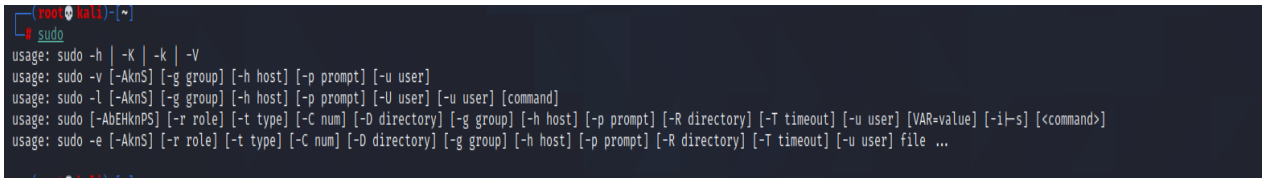


103. pstree:

Description: It displays all the currently running processes in the tree format.

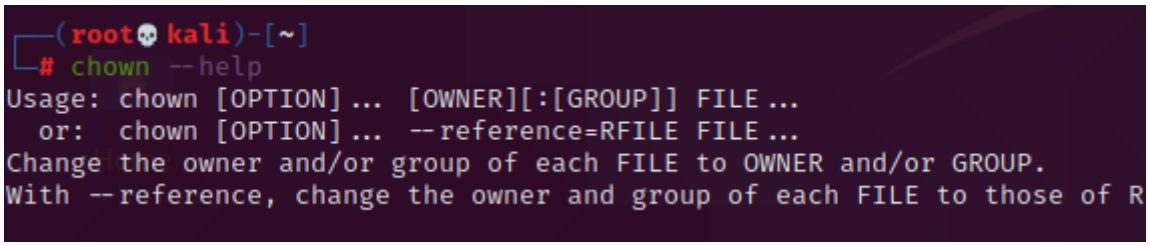
104. sudo:

Description: It is used to run commands as a root user.



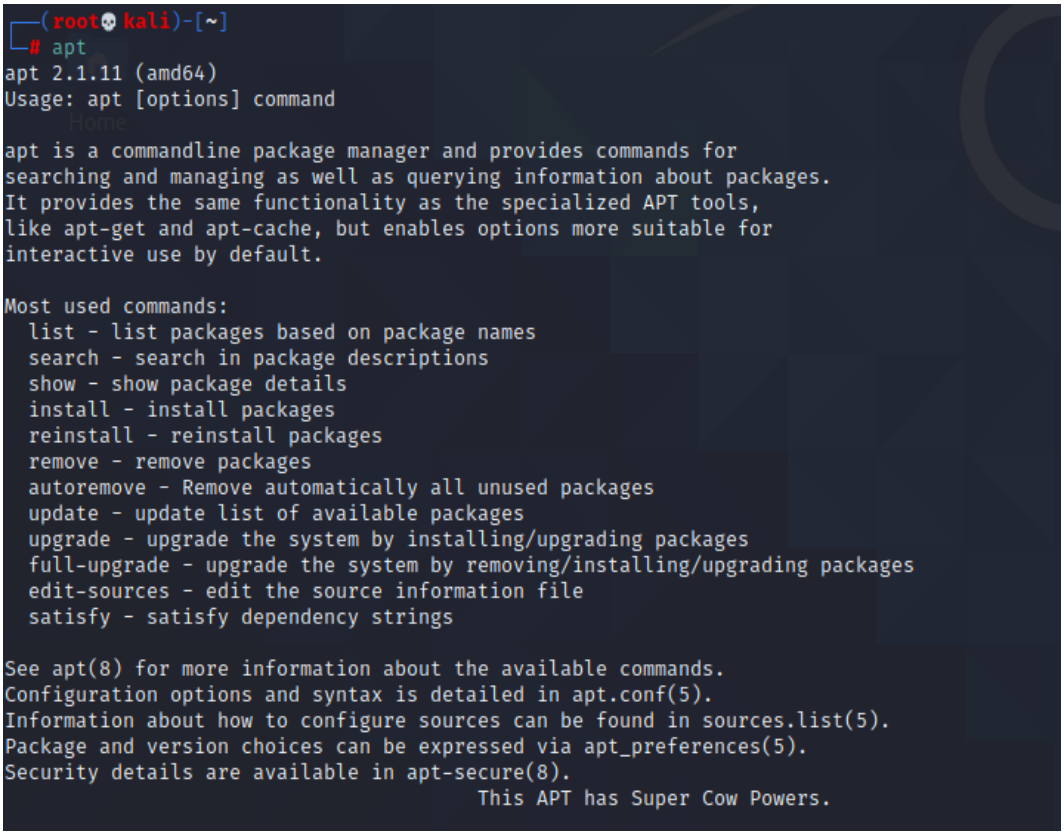
105. chown:

Description: Change the owner or group of each file.



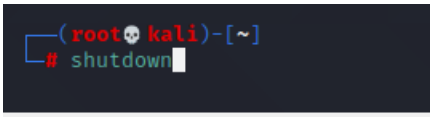
106. apt:

Description: It helps to interact with the packaging system.



107. shutdown:

Description: It shuts down the system.

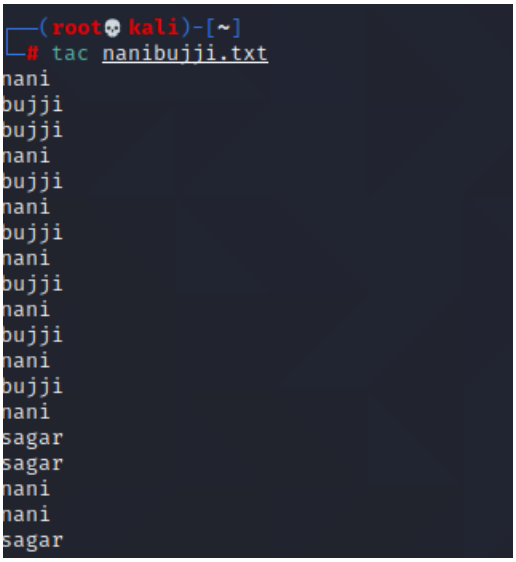


108. wget:

Description: It is an interaction-less command for download of files from web.

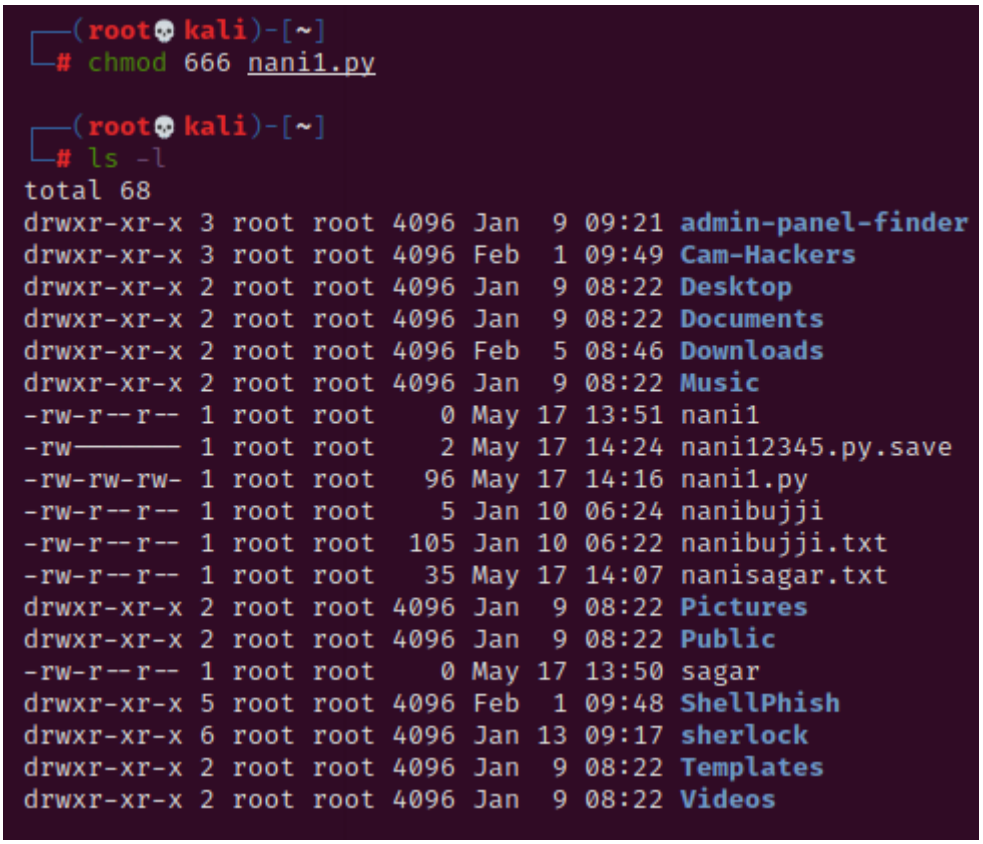
109. tac filename:

Description: It displays the contents of the file in reverse order.



110. chmod 666 file.py:

Description: It helps to change the functional permissions such as read and write for a particular file.



➢ Now, let us know about some basic keys in kali Linux,

- **COPY –** Ctrl + shift + C.
- **PASTE –** Ctrl + shift + V.
- **SAVE –** Ctrl + O.
- **EXIT –** Ctrl + E.

Now, let us go brief into the phases of hacking:

Information Gathering:

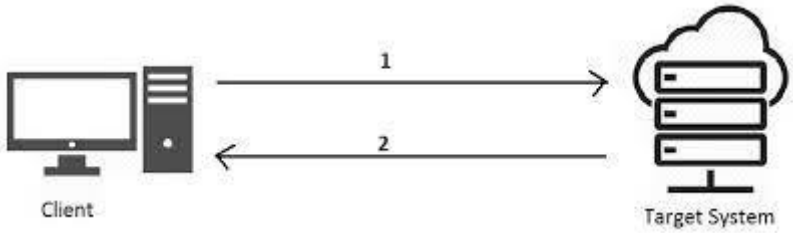
Information gathering is the process in which we gather the information of the target we are going to attack. The information we gather comprises of the strengths and weakness of the victim or target. Mostly, we target on the weakness of the target which is the main thing useful for us to attack easily. It is the starting step of ethical hacking or hacking. The more the information we know, the easier the process of hacking is done. The strengths of the victim are also necessary to be known. The more the information which is against the target, the easier and lesser the time takes to hack the system. This is done by both hacker and ethical hackers i.e., penetration testers and hackers. There are several tools and techniques in this process which help in gathering whole data of the victim with small vulnerabilities. The personal information of the victim is also necessary while hacking. Because, we may need some words relevant to the victim like his favourite person's name or some other information while cracking some type of passwords or keys.

The information gathering is also two types:

- Active Information Gathering.
- Passive Information Gathering.

Active information gathering:

It is like gathering information with direct contact from the target or the victim. Like, talking to the victim, accessing his computer directly, knowing his secrets as his friend.



We can know more information easily without any difficulty in this active information gathering. Because it is easier to get information from a person than getting information from a computer/computer system. The information gathered like names, favourite person names, pet names, system details can be gathered and use these to hack or penetrate into the system of the target.

There are different types in active information gathering:

Everything is part of Social Engineering in active information gathering.

Social Engineering:

Social engineering is the art of manipulating or making their minds exploited and control them with emotions as their close friends and finding their details and personal information. Social engineering is not just like doing it with the software or well knowledgeable persons. It doesn't need much hacking skills, it needs communication skills and tackling skills, dealing with people by estimating their psychology and knowing their weakness and trying to get the maximum data about the victim.

The Social engineering is also comprised of different types:

- Human-based.
- Computer-based.
- Mobile-based.

Human-based:

It is the type of social engineering in which humans do it to gain the information from the victim with different processes and manipulate them. There are different types of processes which humans follow to manipulate the targets or victims. Some of them are like:

- Eaves Dropping.
- Dumpster diving.
- Piggy backing.
- Tail gating.
- Baiting.

a) **Eaves Dropping:** When two people are talking or discussing about the confidential data, if any the person hear, it is called eaves dropping. This is one of the processes of human based social engineering in information gathering. Eaves dropping is hearing others secrets without knowing to them and gathering most information from the data heard. It also involves like the data transferred between two devices or persons is being known or being modified.

This is the technique which exposes most of the secret data without misleading the users.

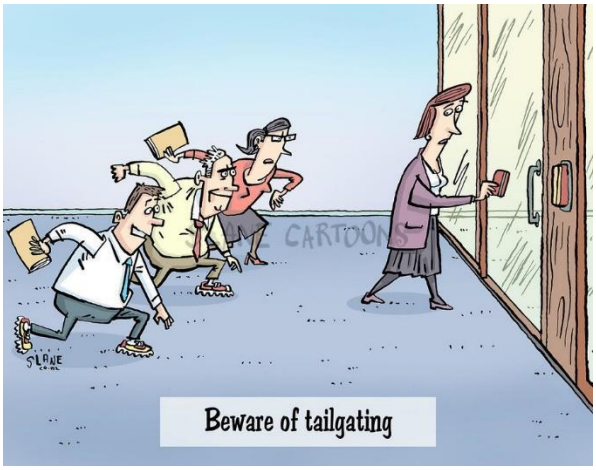
b) **Dumpster diving:** It is a technique in which we check for any sensitive information with the user or the person handling the system. The sensitive or confidential data is very useful for the process of hacking as we could gather the main information like the passwords, usernames, card details, system configurations, IP addresses, wi-fi passwords, etc. All this sensitive information is collected to gather lots of information of the victim to affect him with the attacks they are going to cause in the future. Here, investigating the victim or people related to the victim also come under dumpster diving.
The main technique involved in the dumpster diving is finding the details of the target or victim from the trash/recycle bin. This is like finding gold in the dustbin, but mostly the previous files, old ones are thrown into trash and in computer to recycle bin. This is used as information for the hackers. More information is got from these files easily.

This is an old technique, but most of the times when there is no other option, dumpster diving gives best results.

c) **Piggy backing:** It is technique which is like entering a system or computer or a network with the help of the original user by tagging them with your system. If found that a person is operating or have the official access of the target system/company, then that user is being manipulated and hacked. Then when that person uses the target with his credentials, the hacker just tags the user system with his system. This allows directly access the victim or target without any penetrating the protective layers. It is like a person tags along with another person while entering into a network or company who have the authorised access. This helps the person or hacker to enter a system easily.

This is not at all allowed or encouraged in any company. This is very dangerous even if the company has many protective layers of security.

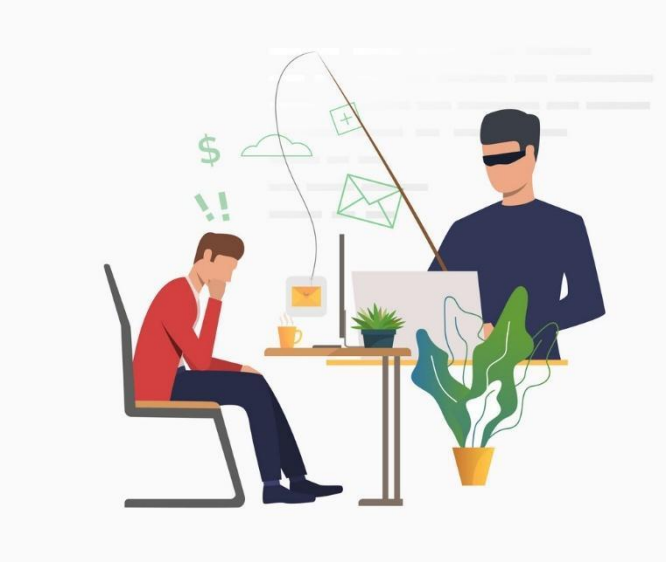
d) **Tail Gating:** It is the technique in which an unauthorised person follows an authorised person to enter a secured area which is prohibited. This is similar to the piggy backing but this is like directly following the person and not tagging him. This allows the person who entered without authorised access, get whole data easily without having to try hard for getting basic data.



Tail gating can be prevented by having security checks, authorisation with multifactor authentication process, etc.

e) **Baiting:** It is like showing a treasure or giving a false promise to make the user of the target system fall for you and grab all the information related to that. The victim's greed is the main weapon for this technique. The curiosity of the victim to open the link sent will be a major power to the hacker to get all the information.

The Victim is fallen or lured into a trap kept for him and all the personal information is grabbed by the hacker who want to gather the information. This is also a technique which is similar to honey coomb technique which is used against the hackers.



This also involves luring a person with spam mails, which contain the links leading to steal the information from the user or target victim. It mostly relies on the lure or greed of the victim. This becomes easy for the hackers, if the victim is tending to greed.

Computer-based:

If the social engineering is done through the computer, then it is called computer based social engineering. It is gathering information using the computer or system. The intruder attacks the weak points of the victim and gather all the information from it. The weak points here are not about the security protection, but to lure the user and his computer and tend to open the link or mail sent by the hacker. This leads to accessing of the system by the hacker. Computer based also comprises of taking the access from the user and silently sending the files required to the hacker's system and clearing the logs.

There are different types in the computer based social engineering:

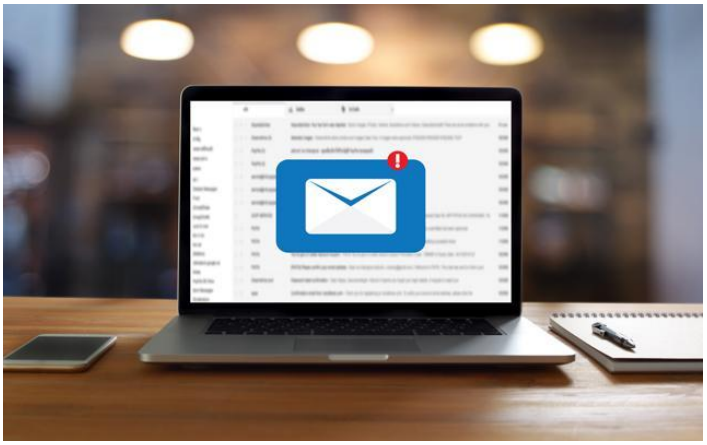
- Phishing.
- Whaling.
- Pretexting.
- Vishing.

a) **Phishing:** Phishing is creating a fake web page which is similar to the original one and making it to redirect to the original site when submitted or used. This doesn't seem like any wrong to the person opened the link, it just feels like submit the details again or just any type of network issues. The person feels like to submit the details again.
Spear phishing: It is the phishing attack done on the particular persons of any company which is the target. Like the victim is the company and main target is also company, but to make the company victim, we need to have an access to the company's accounts which are always confidential and the access is known to few people only. Instead of the bigger targets, this concentrates on the smaller ones like employees, workers, etc.
This is very important to check whether the mail or link is from official site or not. So before believing in any links or mails and clicking on the content in them is not a safe method. This leaks the total information of the user to the person who sent the link. This is also a process of social engineering based on computer.

b) **Whaling:** Whaling is same as phishing but targeted on high professionals who are the main source of information in a company or in any government. This could lead to major information leakage.

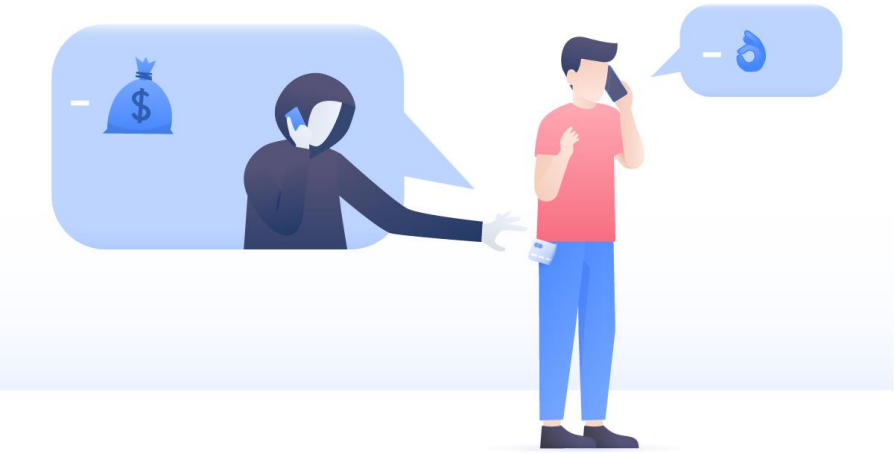
The major difference between phishing and whaling is the targets or victims of the attack. This is also tending the target to open a suspicious email or malicious link. This is very dangerous as the victim will be the higher official of the company like CEO or CFO. In a survey it is proved that 72% of the whaling attacks are done on the CEO of the companies while 36% of the attacks are done on the CFO of the companies and remaining on the other major employees. This shows that the information of the company is easily leaked by the officials as they think that their account is secured.

c) **Pretexting:** Pretexting is a common usage of the social engineering showing a fake message that lures people with the outer appearance. This is a technique of social engineering. The people click on the links which show that the link can give free offers.



These messages may come from social media like Whatsapp, Instagram, Mail, Facebook and some other mediums. This technique which is more useful for information gathering in mass amount and confidential information. The confidential information like passwords, card details can be easily hacked here. The attacker could convince the user or target that the sent mail or message is official one by the banner on the mails and links, but these are created on the names of the original one.

d) **Vishing:** Vishing is an attack from the hackers through voice calls or voice message. It is not like sending any malwares to the mobile. It is like provoking the target or victim to tell the confidential information by creating urgency of the users. This is like saying the victims that they called from your registered sim managers or banks. The users think that the call is from the official people or authorised people and tend to give their details asked. With the communication power of the caller the target doesn't even make to think about the consequences later.



Mobile based:

There are many ways in mobile based social engineering. The spam messages are sent to the mobile and when the users click the links or signup in them the mail and password are stolen by the attacker who sent the link or the spam message. This is like a type of phishing. The mobile based hacking is easier with the adults who doesn't know the basic information and knowledge of a mobile and only use it for making phone calls.

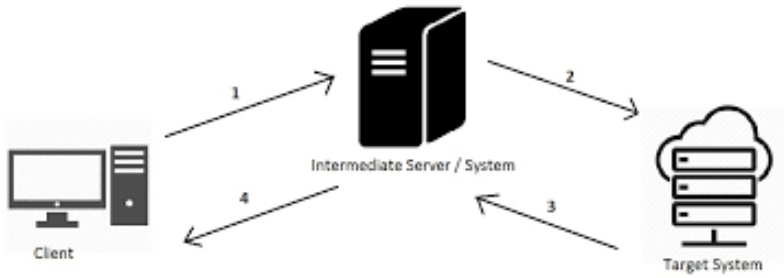
The social engineering is not so difficult even in the minors. The people who give the mobile to children without the child lock, may face a problem when the children click on the messages or links. The source is not easy to be found, but the messages are seen as reliable. So, being careful and protecting your mobile is the only way to save it.

Passive Information Gathering:

Passive Information Engineering is gathering information from the victim or target without knowing to the person or contacting him.

The passive information is all about gathering information using the tools and websites which are embedded with information gathering techniques. The passive information gathering is not only gathering information but also hiding from the user

or victim without recognising the hacker. This information gathering is happened without establishing a contact from the user.



There are many types in passive information gathering:

- Digital Information gathering.
- System Information gathering.
- Organization Information gathering.
- Financial Information gathering.

a) **Digital Information Gathering:** It is also called as network information gathering. Here, the information gathering involves IP addresses, Network zones, Some Websites which are useful to gather information, Network blocks, DNS records, etc. The digital information gathering is a type of information gathering which allows us to gather information which is on the net and can be got with tools using on the internet.

DNS Records: A database which matches the URLs with the correct IP addresses.

b) **System Information Gathering:** The system information comprises of some crucial information like web server name, configuration and its details along with the model number, OS or operating system name and its details, location of the system or the user, etc. These details come under the system information gathering. With this, the attacker can determine the tools to be used and need not to try a vast number of tools to attack the system or computer.

The system information is very crucial because, this is the main information to hack any information from that computer. Protective measures for the servers and systems must be taken.

c) **Organization Information Gathering:** The details of the company like the some more crucial part like emails of the company and its employees. The faxes, phone numbers, locations and other information comes under the organization information. This information is gathered comprises of the other information like organization establishing date and other information. This is used for sending fake mails as said before in active information gathering.

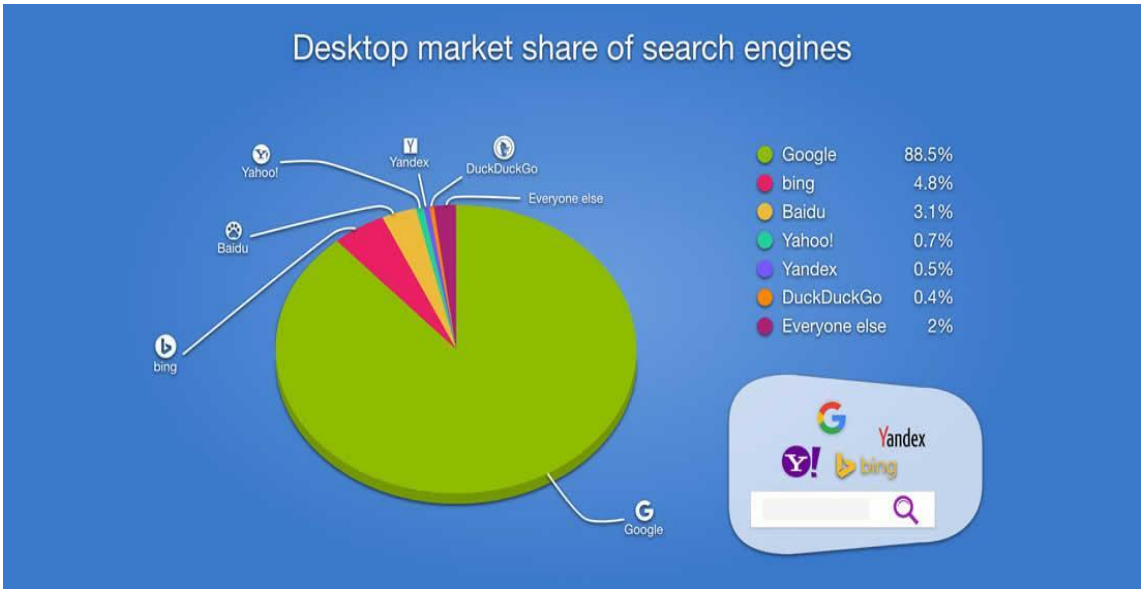
d) **Financial Information Gathering:** The financial information contains the details like card details, account details, web technologies, sub domains and other information. The financial information is very useful for the hacker to damage the financial background of the company. The card details or the account details of the company income sources and its information is the source here. With at we can totally damage the company ad ruin it.

The information gathering is done with the help of the internet search engines in a vast manner. Because every company registers its profile on the internet with the little information of the company like the goals, targets of the company, the process of the company, etc. The search engines are entirely a big source for information gathering of any target. Some of the search engines are: **Google, Yahoo and DuckDuckGo, Bing, Ask, Yandex, Baidu,** etc. These are the major search engines with vast information in it.

The search engines are not only source of information but the source of finding different types of tools to gather other type of information. Like, some other information gathering tools in hacking.

The search engines are as below:

The search engine users around the world mostly use these four websites, there are few other sites but majority uses only these. The surveys around the world shows the results that these search engines are the majority likes ones. The interface of these websites is mostly better than other sites. There are some search engines which definitely have specific features than others. The search engines market share is totally taken by the market giant ‘GOOGLE’. This comprises of almost 90% of the market share in the search engine index. This is drastically hanging and the search engines like DuckDuckGo are coming into use by increasing their market share to 0.4% and Bing to 4.8%. There are other sites which are drastically decreasing its usage like Baidu which has fallen to 3.1%, Yahoo is risen to 0.7%. Yandex has fallen from a bigger market share to 0.5%. Everything else is the remaining share which is not even 0.1% of the market share.



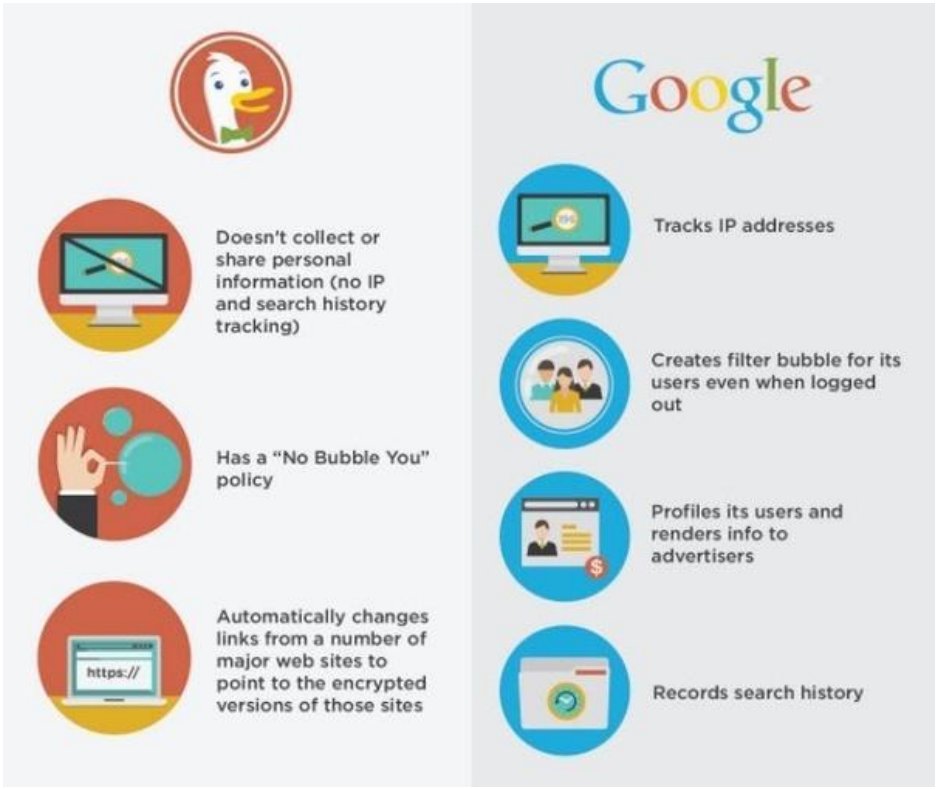
The source of income of these market giants is advertisements. The more the engagement with the advertisements by the user, the more the income the search engines get.

Google: It is the present market giant in the internet which holds almost 90% of the market. It is designed to store the IP addresses of the user and also track them. It also stores the user information. Based on the information we search it shows the advertisements to us in the daily life. It is also linked up with many social media platforms, which even shows the advertisements there. This is mostly only for the quick and mostly relevant responses given for a search and gives a lot of trash searches also. Google processes around 3.5 Billion searches a day. This is a huge number obviously. Google has some privacy policies for protecting from the malwares, ransomwares, viruses and other dangers in the internet.

One of the reasons to avoid the usage of google by some people is that the privacy. It also records the search history.

DuckDuckGo: DuckDuckGo is a search engine which is used by most of the people who want to keep their searches safe. The DuckDuckGo doesn't record any searches. It does not even store he history of the person. There is no profiling in DuckDuckGo. This is the unique feature apart from others. The safest search engine ever is

DuckDuckGo. Because it does not even analyse or use the searched information for advertising. The DuckDuckGo still depend on the income from the advertisements. It does not have any other source of income. It does show advertisements not related to the user data which is searched, but different ones. The DuckDuckGo does not stop any malwares, viruses from entering into the computer or system. It shows the search results which are only essential and sometimes it shows irrelevant results. This is totally secured website. The total details will be in privacy without even knowing to the owner of DuckDuckGo. The DuckDuckGo is designed in way that not to track the details of the IP addresses and locations of the users. This is the best feature which is attracting people.



Google Dorks: Google dorks is technique of using some search strings which are helpful for advanced search strings. These are used to find the very relevant information we want with just small key words with our original searches. These are generally used by ethical hackers and hackers to save the time and search as fast as the internet speed available. It is open for all the people with basic knowledge, it is just unusual thing but not any illegal one. This Dorking helps the hackers or ethical

hackers to find the information very fast and not any hacking technique. This is just using the techniques available in open source as advanced search commands.

The Google Dorks are like small command in the vast information and data base of the Google.

Some of them are as below:

Let us assume now '**$**' is the required type of sites we want. Then,

- The dork here is **inurl: .$**

  Suppose,

  - For websites of Pakistan inurl: .pk
  - For United Kingdom inurl: .uk
  - For United States inurl: .us
  - For Australia inurl: .au
  - For Canada inurl: .ca

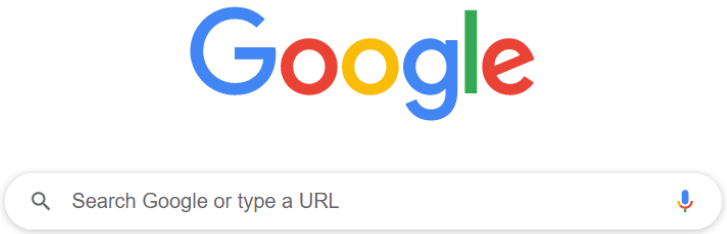
- For a book we need, The Dork is like **Book: Book name**
- For login sites we need, The Dork is **inurl: login**
- For signup sites we need, The Dork is **inurl: signup**
- For college websites, The Dork is **inurl: colleges**
- For the movie we need, The Dork is **inurl:<space>.movie name**

GHDB: (Google Hacking Data Base) This is the data base containing the search terms containing the sensitive data which is brought out or exposed by vulnerable servers and web applications. It is first launched by Johny Long in the year 2000 to help the penetration testers.

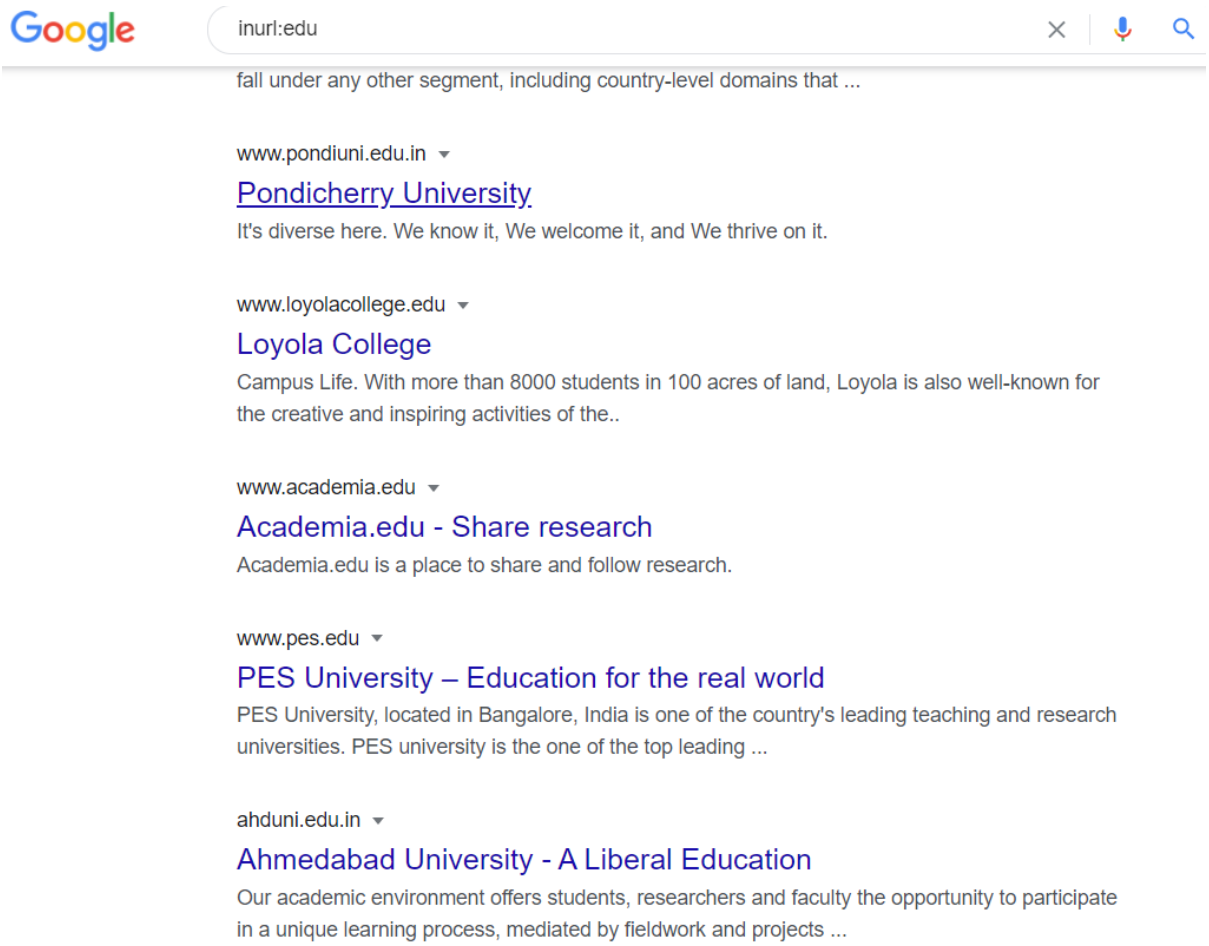
Now let us apply the we known:

I. Finding college sites using google dorks:

Step 1: Open Google Chrome



Step 2: With the help of google dorks like shortcuts get the websites of the colleges and educational institutions. Here the DORK is **"inurl:edu"** or **"inurl: .edu".** We get all the websites ending with 'edu' which are educational institutions. Then note down the 30 college websites you want.



1. **MVSR Engineering college:**
   Link:
   https://www.mvsrec.edu.in/index.php?option=com_content&view=article&id=648&Itemid=1228

2. **REVA University:**
   Link:
   https://reva.edu.in/

3. **Kautilya Institute of management and Research**
   Link:
   https://jspmkimr.edu.in/

4. **Loyola College:**
   Link:
   https://www.loyolacollege.edu/

5. **Pondicherry University:**

   Link:

   https://www.pondiuni.edu.in/

6. **Chitkara University:**
   Link:
   https://www.chitkara.edu.in/

7. **Andhra University:**
   Link:
   https://www.andhrauniversity.edu.in/

8. **PES University:**
   Link:
   https://www.pes.edu/

9. **Amity University:**
   Link:
   https://www.amity.edu/

10. **Sastra University:**
    Link:
    https://www.sastra.edu/

11. **Alliance University:**
    Link:
    https://www.alliance.edu.in/

12. **Jadavpur University:**
    Link:
    http://www.jaduniv.edu.in/

13. **Azim premji University:**
    Link:
    https://azimpremjiuniversity.edu.in/

14. **Mumbai Educational Trust league colleges:**
    Link:

https://www.met.edu/

15. **APJ Abdul kalam Technological University:**
    Link:
    https://app.ktu.edu.in/

16. **Anna University:**
    Link:
    https://www.annauniv.edu/

17. **National Institute of Design:**
    Link:
    http://www.nid.edu/

18. **National institute of Technology, Trichy:**
    Link:
    https://www.nitt.edu/

19. **JBAS college for women:**
    Link:
    https://www.jbascollege.edu.in/

20. **Shiv Nadar University:**
    Link:
    https://snu.edu.in/

21. **Ashoka University:**
    Link:
    https://www.ashoka.edu.in/

22. **Thapar Institute of Technology and sciences:**
    Link:
    http://www.thapar.edu/

23. **Jindal Global Institute of Eminence Deemed to be University:**
    Link:
    https://jgu.edu.in/

24. **Professor Jaya shankar Telangana state Agricultural University:**
    Link:

https://www.pjtsau.edu.in/

25. **Fergusson College:**
    Link:
    https://www.fergusson.edu/

26. **Punjab Agricultural University:**
    Link:
    https://www.pau.edu/

27. **Sardar Patel University:**
    Link:
    http://www.spuvvn.edu/

28. **Babasaheb Bheemarao Ambedkar Bihar University:**
    Link:
    https://brabu.edu.in/

29. **GITAM University:**
    Link:
    https://www.gitam.edu/

30. **DIT University:**
    Link:
    https://www.dituniversity.edu.in/

Now, try it with the country websites you want:

I. **Finding Australia websites using google dorks.**
   Here the Dork is **"inurl: .au"**

1. https://www.studyinaustralia.gov.au/English/Australian-Education/Universities-Higher-Education/list-of-australian-universities

2. https://www.psa.org.au/

3. https://www.awe.gov.au/news/media-releases

4. https://www.sa.gov.au/topics/energy-and-environment/using-saving-energy/easy-energy-saving-tips

5. https://www.environment.gov.au/protection/publications/hazardous-waste-australia-2017

6. https://www.care.org.au/donate/

7. https://bankaust.com.au/

8. https://www.auda.org.au/

9. https://www.amnesty.org.au/

10. https://www.visionaustralia.org/donate

11. https://www.littil.com.au/

12. https://www.arpansa.gov.au/understanding-radiation/radiation-sources/more-radiation-sources/sun-exposure

13. https://auspost.com.au/about-us/about-our-site/responsible-disclosure

14. https://www.accc.gov.au/business/treating-customers-fairly/offering-warranties

15. https://www.abs.gov.au/methodologies/weekly-payroll-jobs-and-wages-australia-methodology/week-ending-5-september-2020

16. https://www.betterhealth.vic.gov.au/

17. https://www.aph.gov.au/search/url/Inquiry/26171_24106_

18. https://www.tga.gov.au/medical-devices-ivds

19. https://digitaltreasury.com.au/australian-guest-blogging-sites/

20. http://www.geoscience.gov.au/web-services

21. https://www.dha.gov.au/

22. https://www.animalsaustralia.org/
23. https://www.cleanupaustraliaday.org.au/become-a-changemaker

24. https://www.greenpeace.org.au/donate

25. https://www.news.com.au/national

26. https://www.swinburne.edu.au/library/search/databases/

27. https://www.specialistaustralia.com.au/why-is-the-skin-cancer-rate-higher-in-australia/

28. https://myliquoronline.com.au/

29. https://www.netregistry.com.au/domain-names/registration/

30. https://www.wesleycollege.edu.au/community/support-us/donate/donation-terms-and-condition

31. https://www.sydney.edu.au/news-opinion/news/2020/09/28/australians-want-to-work-from-home-more-post-covid.html

32. https://invasives.org.au/donate/

33. https://www.jlg.com/en-au

34. https://www.allassignmenthelp.com/au/

35. https://www.amsa.gov.au/about/regulations-and-standards

36. https://www.acoss.org.au/wp-content/uploads/2016/10/Poverty-in-Australia-2016.pdf

37. https://www.osteoporosis.org.au/sites/default/files/files/vitdconsumerguide.pdf

38. https://www.sustainability.vic.gov.au/You-and-your-home/Live-sustainably/Save-water

39. https://amhonline.amh.net.au/

40. https://www.nielsen.com/au/en/client-login/

41. https://www.dfat.gov.au/people-to-people/australia-awards/Pages/australia-awards

42. https://www.seaviewhs.sa.edu.au/

43. https://www.dfat.gov.au/people-to-people/australia-awards/Pages/australia-awards

44. https://www.seaviewhs.sa.edu.au/

45. https://zibdigital.com.au/digital-marketing-agency-melbourne/

46. https://signartqld.com.au/inurl-essay-writing-services

47. https://www.oxfordshop.com.au/

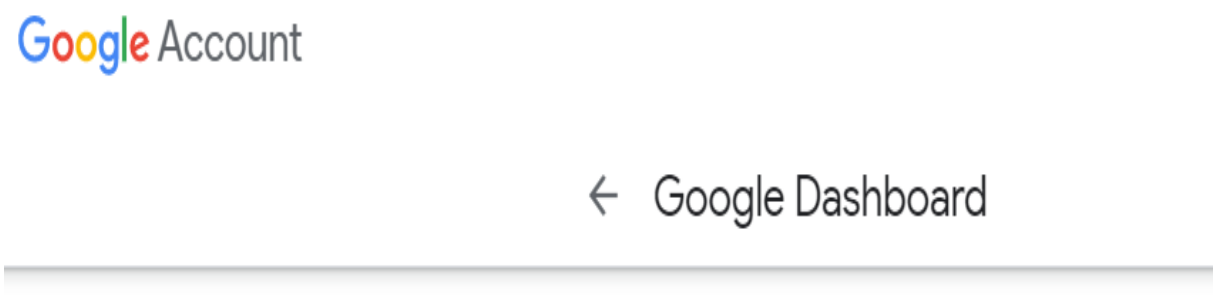
48. https://moodle.telt.unsw.edu.au/

49. https://forum.coie.com.au/community/profile/betsen6180143/

50. https://www.industry.gov.au/sites/default/files/2018-12/australias-tech-future.pdf

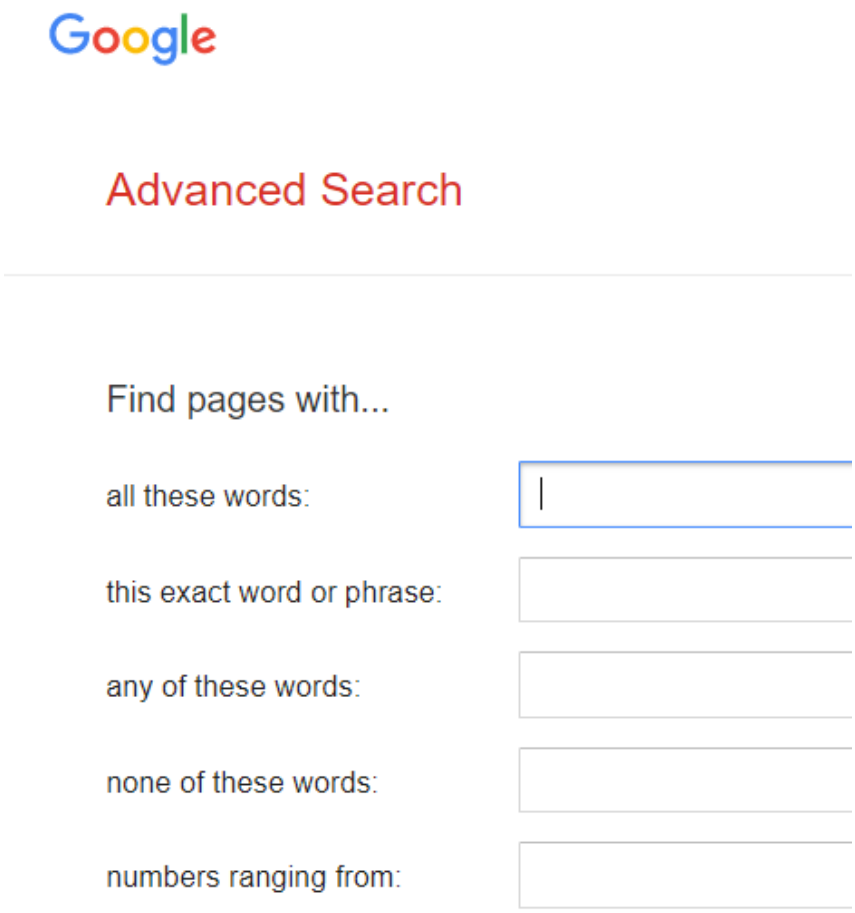
These are the different ways google dorks are used as advanced search technique. Now, let us know some more information about google.

Google Dashboard: The google dashboard is the place where the mail generate for us is being registered and all the information linked to google is being stored. The Google not only stores the information but also tracks the location of the places where mobile is moving and stores that data in the “My Activity” section of location history. The Google Dashboard can be linked with the contacts, photos and other details of us. This information is stored permanently and even if the device is lost, we can open and access the information in any other device with our mail and its password.



This is really a cool one. The storage limit for any person is 15GB which is for free and if needed more space, then it is payable. This feature enables us to store a lot of data within the google. Google Dashboard also has many other cool features to access. If the mobile is lost and need to find it, we can open our mail in any other device and find the location of our phone with "Fond my device" with location ON in the mobile and if not, it shows the last location, when the location setting is turned off. This feature is very useful for information gathering if the hacker just knows the mail and password of the victim.

Google Advanced Search: Google Advanced Search is a detailed method of searching in which we get vast relevant information compared to normal searches. Here we can decide the type of results we want by just filling the slots given like "**Exact word"** to be in the search result, "**All these words"** which are to be in the results. The google search results are not like any other ones but can even manage the location or country of the results the search belong to. For this technique, the google contains some advanced and special operators designed.



For the advanced search use the link: https://www.google.com/advanced_search

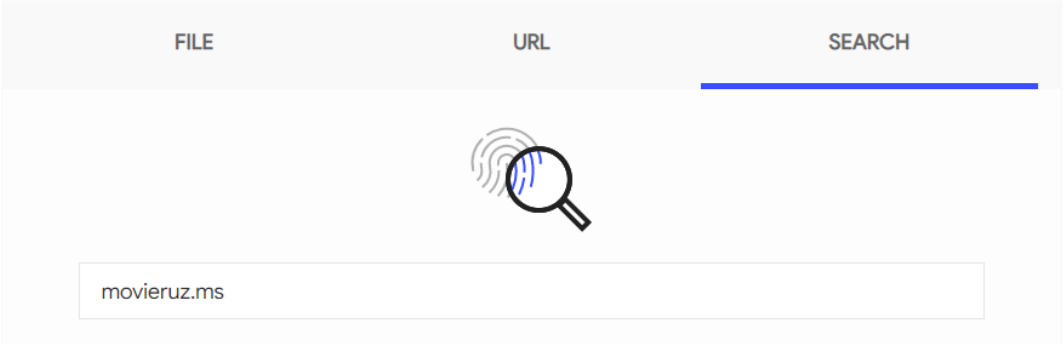
This is link for advanced search in google.

- ☐ There is small shortcut for directly getting the images relevant to the search we type.

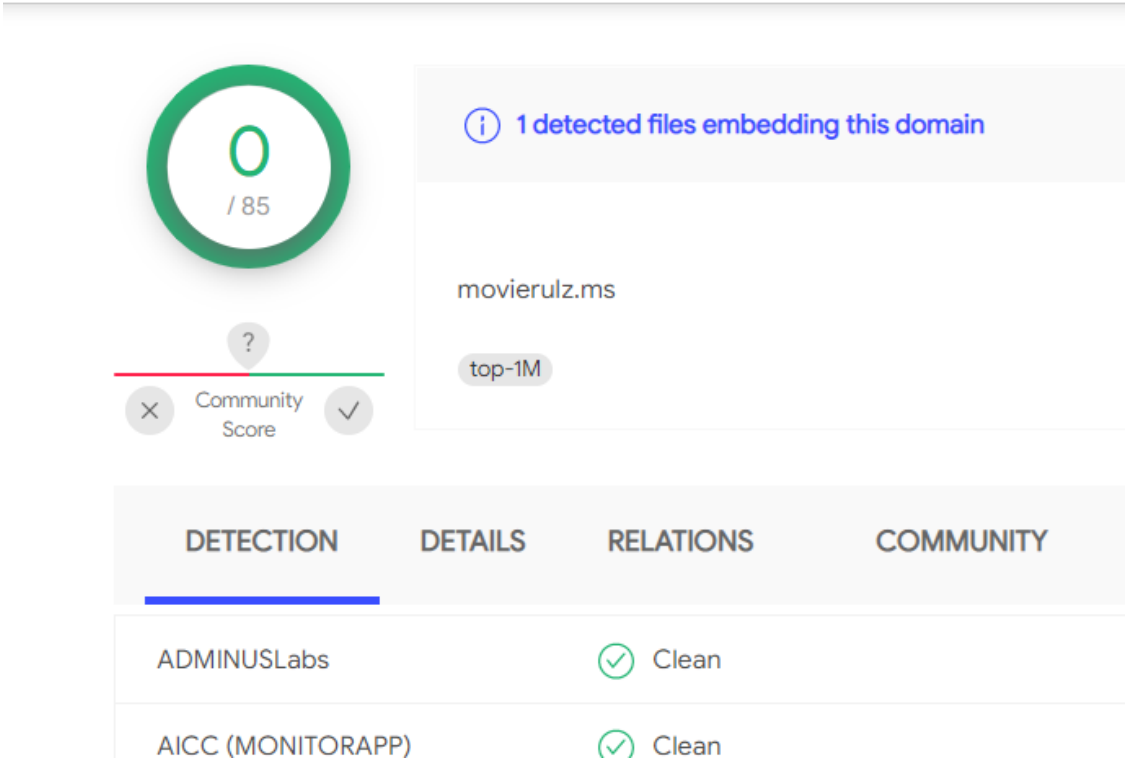
  Use https://images.google.com/ to get a terminal which directly gives the image results which are very useful and very relevant.

☐ There is tool in the google to find the suspicious files or links or applications and searches. If there is any malicious file or harmful virus present in the file, link or search we submitted, then it identifies it and shows us about it.
www.virustotal.com

This tool is "**VIRUS TOTAL**". This identifies all kinds of viruses which are in use until the date of update of the tool. This is very useful one when using some unknown application, opening unknown files, etc.
Let us have a glance on this with "movierulz.ms".



If there are any malicious or harmful file embedded in it, it identifies and displays.



Even if there are any files embedded in the search or uploaded file, it shows as file found embedded as shown above.

Google Earth: It is a terminal which shows the entire earth, any where which are the public locations and there are some locations which can't be seen in the Google Earth which are unauthorized places to the public like Area 51. The google earth is

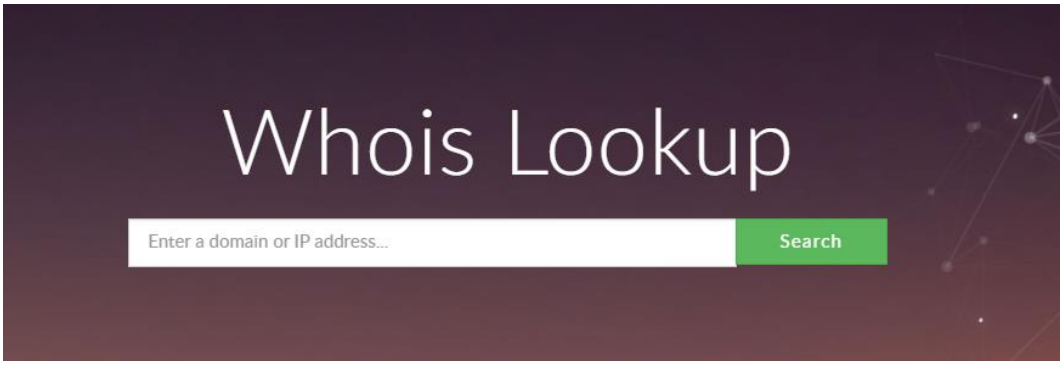
completely different which shows the live earth which is just a few minutes different than the real time. It shows fully HD locations, if the network to the system is good. This can be used in “information gathering” which helps to know the location of the target company we need to find.

There will be an earth display shown we can zoom and search whatever the location we want to see on the earth. We can also search the location we want in the search bar.

Let us discuss about some of the tools which can be used on the internet and some tools which can be downloaded for **Information Gathering.**

1) **Whois lookup**

"Whois" is a tool for gathering the information of any website/URL.



This gives the information about the

- Domain name of the website.
- Gives the information of starting date of the website and updated date of the website.
- Server hosting company name is also displayed here.
- The registered ID of the website is also shown along with the user ID of the customer.

But for the website which have the Whois vulnerability, the excess information other than these like:

- Server Names.
- Server locations.
- Network names.
- Contact and mail of the developer.
- Developer company name.
- Tech Contact.
- Address of the company with location.
- IP Address and IP Location.
- Server type.
- Response code.
- Registrar.
- Tech name, country, state, city.

This gives most of the information of the website if there is Whois vulnerability. This is one of the tools which gives the information about the website, so that the hackers or penetration testers.

This is website which doesn't have the Whois vulnerability.

```
Domain Name: kitsguntur.ac.in
Registry Domain ID: D414400000000513758-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2021-03-31T06:08:50Z
Creation Date: 2016-03-21T04:27:48Z
Registry Expiry Date: 2022-03-21T04:27:48Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: KKR & KSR Institute of Technology & Scie
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
```

This is website which has Whois vulnerability.

```
Domain Name: VASAVIDEGREECOLLEGE.COM
Registry Domain ID: 1712499128_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2021-04-10T03:05:24Z
Creation Date: 2012-04-10T11:01:12Z
Registrar Registration Expiration Date: 2022-04-10T11:01:12Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientT
Registry Registrant ID: Not Available From Registry
Registrant Name: Ravindra
Registrant Organization: Saru Soft Technologies
Registrant Street: Sumateja Residency,  2/12 Brodipet, Guntur
Registrant City: Guntur
Registrant State/Province: Andhra Pradesh
Registrant Postal Code: 522007
Registrant Country: IN
Registrant Phone: +91.08632232829
Registrant Phone Ext:
Registrant Fax: +91.9949842829
Registrant Fax Ext:
Registrant Email:  ravindra.sarusoft@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Ravindra
Admin Organization: Saru Soft Technologies
Admin Street: Sumateja Residency,  2/12 Brodipet, Guntur
```

With the Whois Tool details we can find the websites which have the SSL/TLS certificate availability.

SSL/TLS certificate: (Secure Sockets Layer) (Transport Layer Security)

It’s the technology which is useful and standard for keeping internet connection secure and safe guarding the sensitive and confidential data that I being present in the website and is connected to the data base which address is inked to website. This enables to prevent the cybercrimes on the website that is with SSL certificate. It ensures that the data being transferred from one computer to system or computer to computer is being encrypted bit wise. It has the algorithm to transmit the data from the server to client.

The SSL certificate must be under went a renewal every year to make it safe. The expiry data of the certificate is completed for a year.

☐ The websites with SSL/TLS certificate are shown as below, the expiry date is not yet completed.

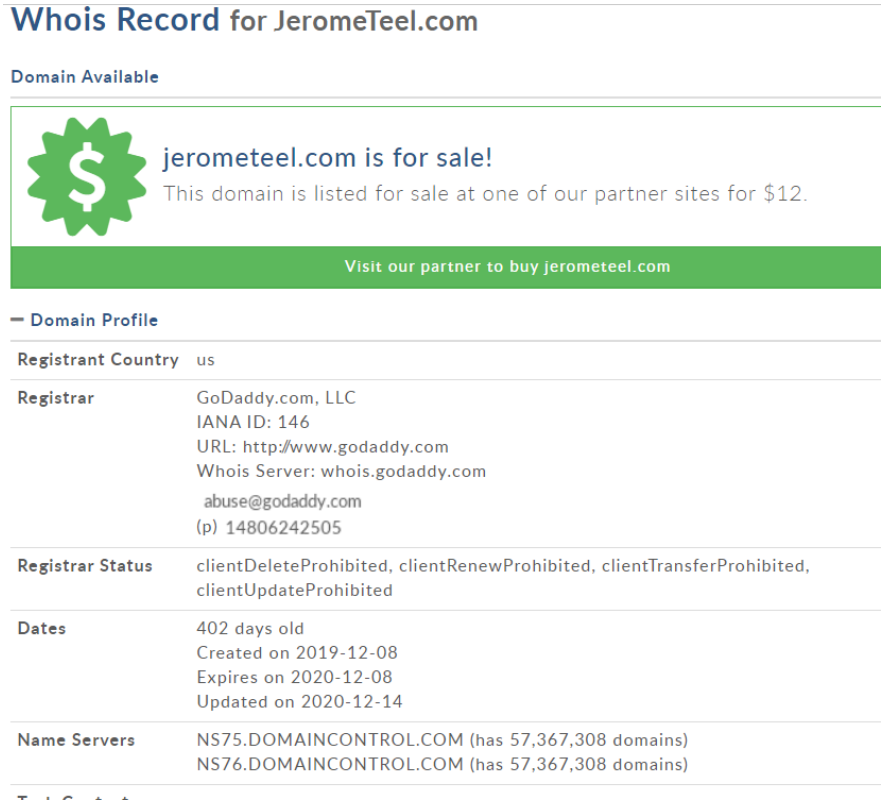
Registrant	REDACTED FOR PRIVACY
Registrant Org	KKR & KSR Institute of Technology & Sciences
Registrant Country	in
Registrar	ERNET India IANA ID: 800068 URL: http://www.ernet.in Whois Server: —
Registrar Status	ok
Dates	1,888 days old Created on 2016-03-20 Expires on 2022-03-20 Updated on 2021-03-30
Name Servers	
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, RED FOR PRIVACY (p) x (f) x
IP Address	45.35.47.173 - 7 other sites hosted on this server
IP Location	- England - London - Psychz Networks
ASN	AS40676 AS40676, US (registered Feb 26, 2008)

☐ There are few websites without SSL/TLS certificates Some of those are:

1) Naisang.com:

Registrant Country	us
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	4,418 days old Created on 2008-12-09 Expires on 2020-12-09 Updated on 2020-12-14
Name Servers	NS43.DOMAINCONTROL.COM (has 57,367,308 domains) NS44.DOMAINCONTROL.COM (has 57,367,308 domains)
Tech Contact	—
IP Address	34.98.99.30 - 2,441,993 other sites hosted on this server
IP Location	- Missouri - Kansas City - Google Llc
ASN	AS15169 GOOGLE, US (registered Mar 30, 2000)
Domain Status	Registered And Active Website

☐ **JeromeTeel.com**



Whois Record for JeromeTeel.com

Domain Available

jerometeel.com is for sale!

This domain is listed for sale at one of our partner sites for $12.

Visit our partner to buy jerometeel.com

Domain Profile

Registrant Country	us
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	402 days old Created on 2019-12-08 Expires on 2020-12-08 Updated on 2020-12-14
Name Servers	NS75.DOMAINCONTROL.COM (has 57,367,308 domains) NS76.DOMAINCONTROL.COM (has 57,367,308 domains)

☐ BataNBricks.com:

Whois Record for BatsNbRicks.com

Domain Available

batsnbricks.com is for sale!

This domain is listed for sale at one of our partner sites for $12.

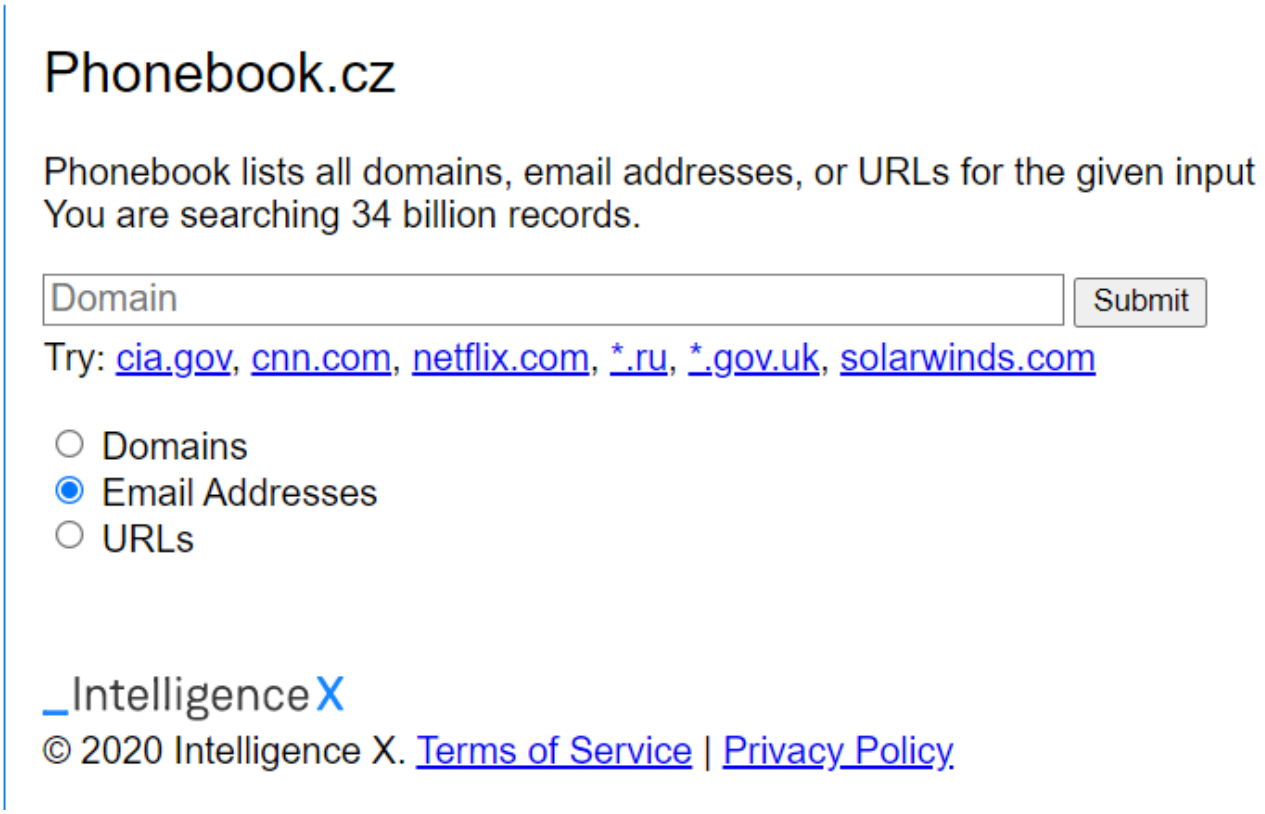
Visit our partner to buy batsnbricks.com

Domain Profile

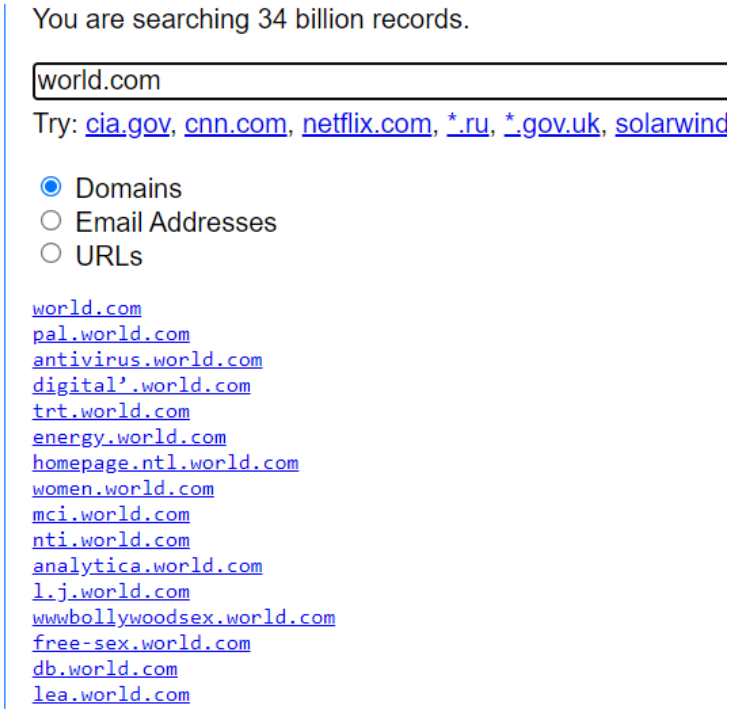
Registrant Country	us
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	766 days old Created on 2018-12-09 Expires on 2020-12-09 Updated on 2018-12-09

2) Phonebook.cz:

The Phonebook.cz is used to gather the all the emails, mail addresses, URLs, sub-domains, domain names, with expected ending like .net, .com, etc. Much information needed can be gathered here with a single click.



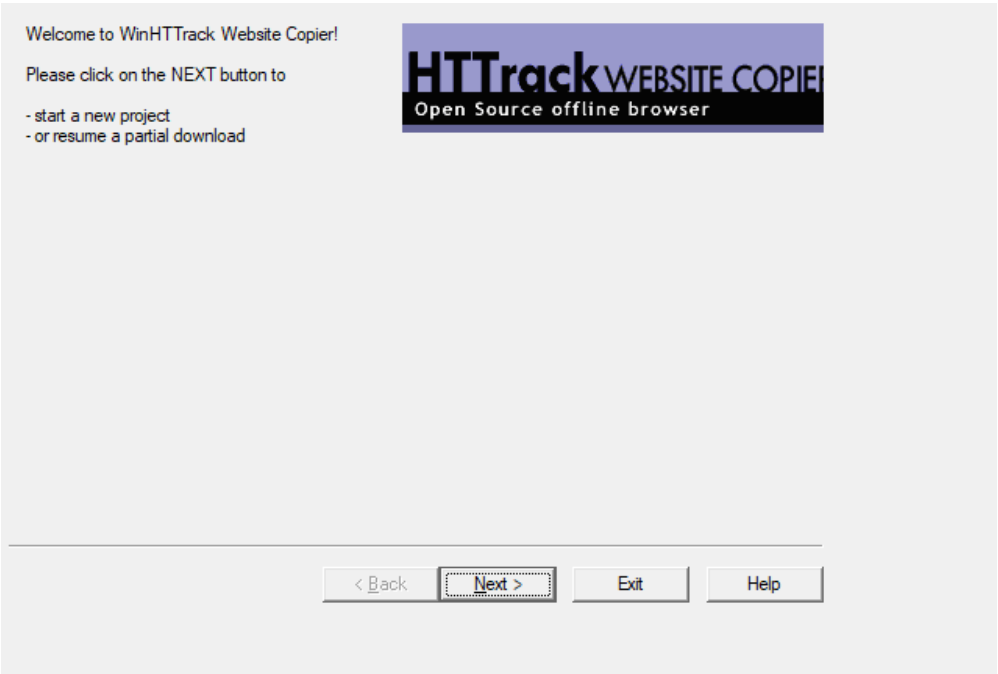
There will a domain typing the word which must be in the results. The results will be relevant to the word we type and with the word we type.



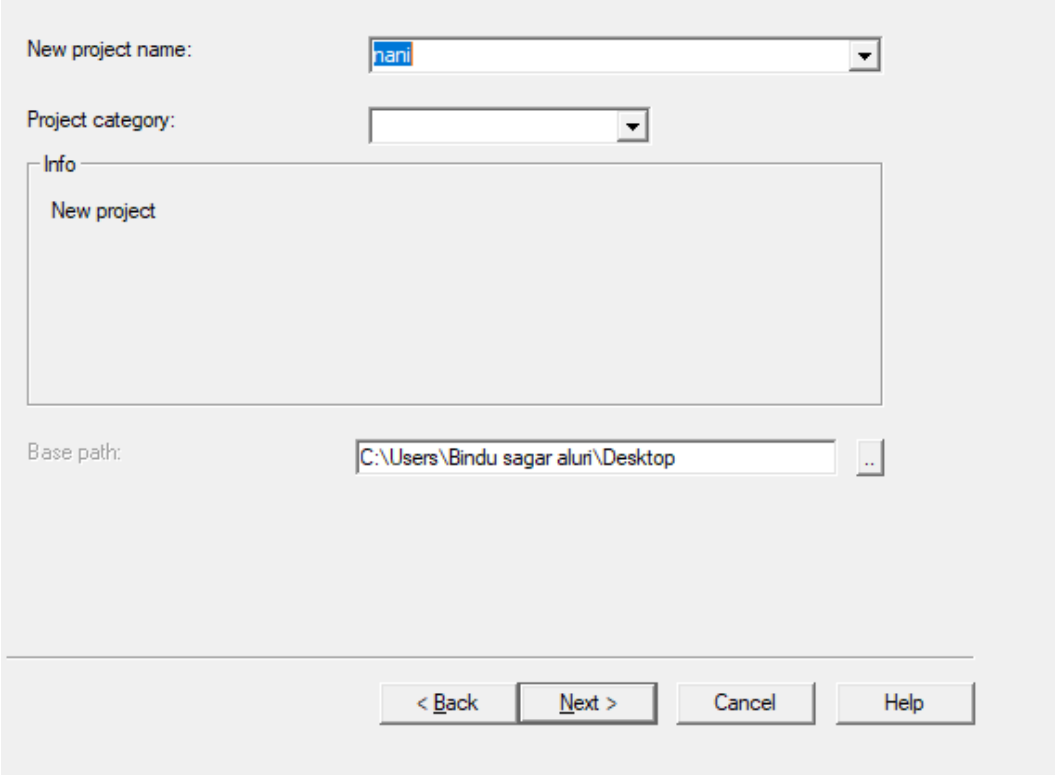
3) HTTrack:

HTTrack is a free tool which is used to download a web page to our local server and it is very easy to use with an offline browser facility. It enables us to download a WWW (World Wide Web) into a file or document or directory. It gets the code which is at the front end like HTML, CSS, Java script, etc. And the code like java, etc. into out local documents where we want to download it.

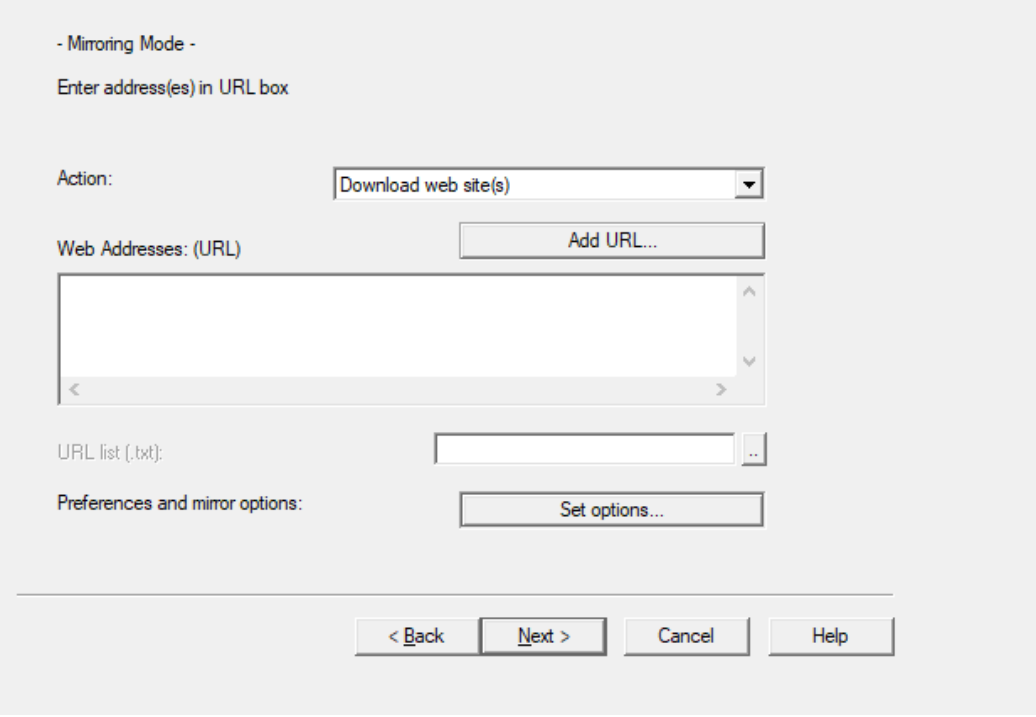
The HTTrack is a tool used as a website copier. This tool as said before downloads all types of the code, files in the given name of the domain or website URL.



This is the main page to start the HTTrack. Now, Click on **Next.** We can start the website copying.

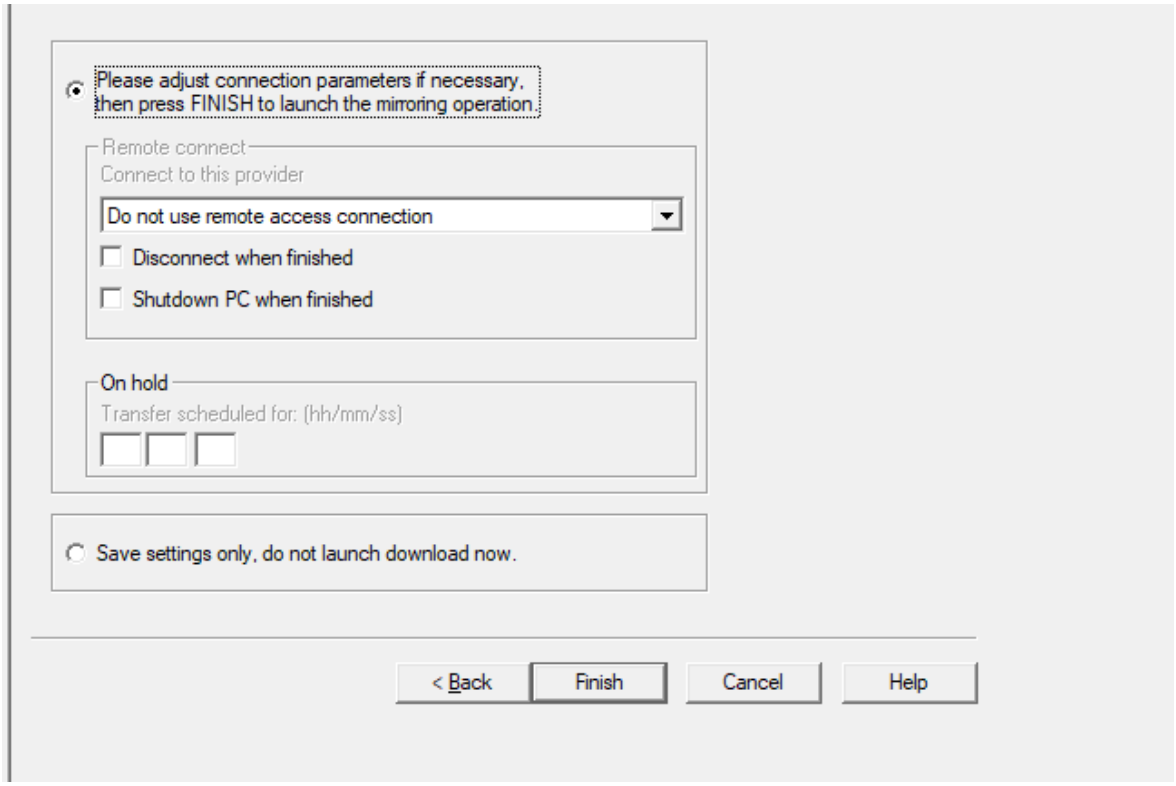


Here allot a project name and click on next to paste the website URL. Here you can even give a project category. We can also decide where to download the document in the computer.

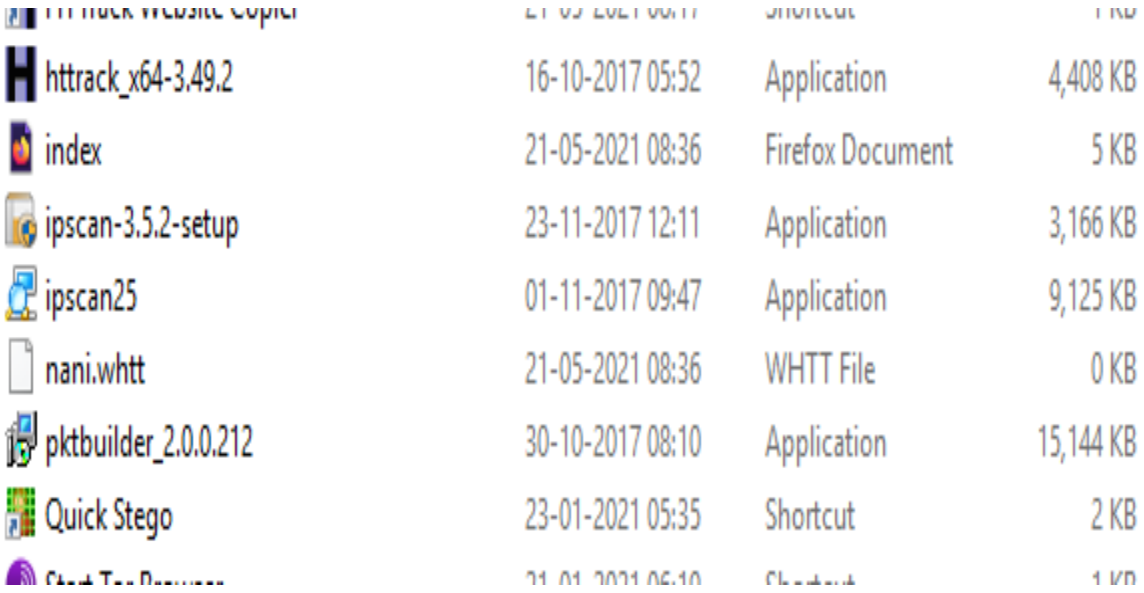


Paste the website address in the space given as web address (URL). And click on next. We can decide the action to be done like downloading website, downloading website and questions, downloading separate files of the content

in the website. We can even decide the proxy to be used with some more additional options.



Now, Finish the process of downloading the content from the website. I chose the website www.kitsguntur.ac.in .



We can see the downloaded file with the name nani.whtt. The HTTrack is easier to use and the majority information hidden in the website and outer website code. We need to stop the Windows Firewall before using it.

4) GitHub:

GitHub is code hosting platform for controlling and collaborating with the projects around the world and websites. The GitHub also enables people from all over the world to work on the same projects and get the results. This also enables companies register on the site to make unknown ethical hackers work on their site to find the vulnerability. GitHub is like a "**Heaven"** for the ethical hackers and penetration testers. GitHub is also a free for its basic services like to host open-source projects. These free accounts on GitHub enables the ethical hackers to show their credibility and talent. This also enables the ethical hackers to earn.

It is an organization which does not have any middle men. It means all the people who work on GitHub projects are managers and also employees. It is an open source. For person it is free for the basic tools. For team it is of some cost of 4$ per month for registering. The Registration for an enterprise is also available for 21$ per month. It is available with all high-end tools and lot of information which can be accessed.

GitHub the web platform used for controlling and collaborating. It simplifies all the processes involved in the collaborating. This is very easy in GitHub to team up and work together with the people across the world. This is not only a

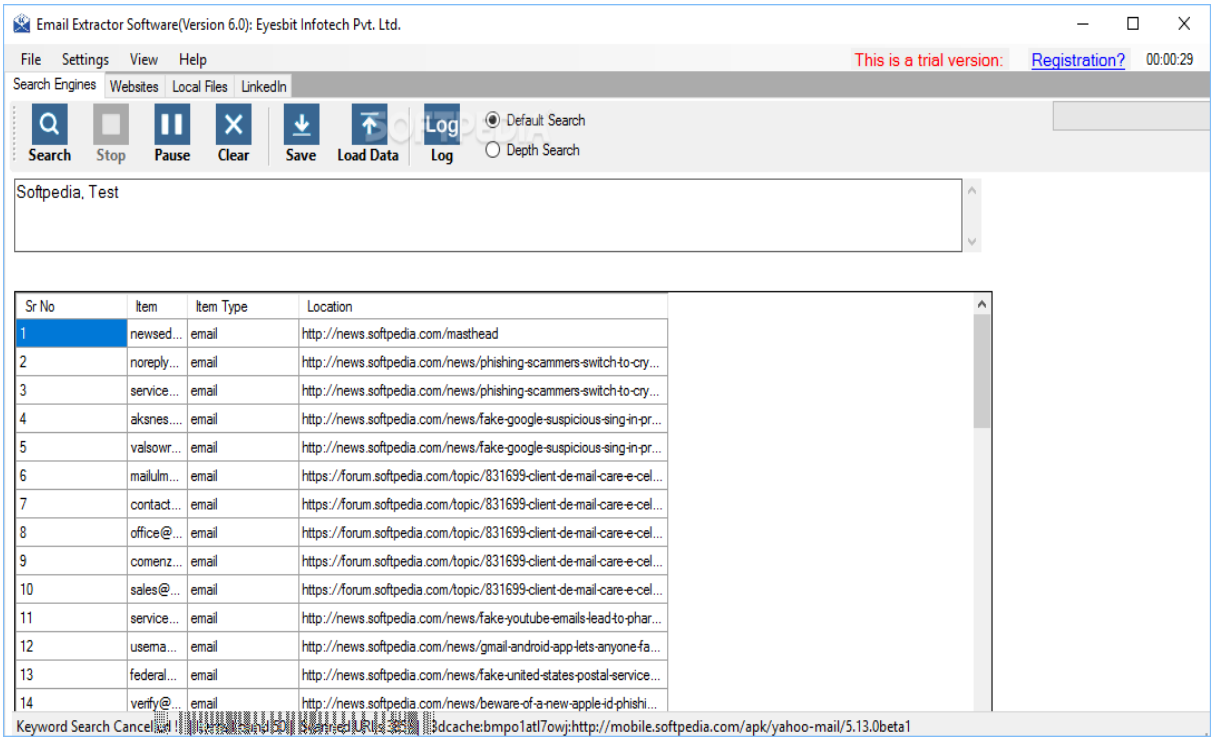
collaborating problem but also can share the work details clearly with the team mates which are being collaborated with us at the start. The GitHub allows us to work and even merge the documents online which enables all the team members who work on the same project could see the details of all the work of the employees.

5) **Email extractor Pro:**

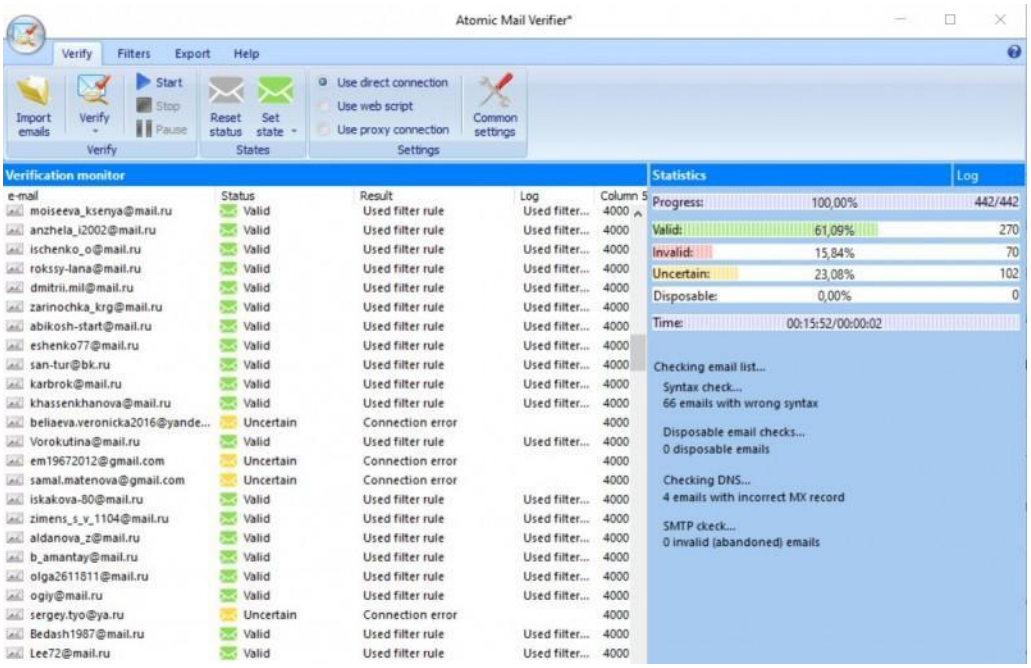
Email Extractor pro is used for conducting email marketing campaigns. It is impossible to collect emails in a large number. To extract large no of emails or addresses, we need a technique to grab the data. The Email extractor helps in grabbing the emails using the files from mailbox itself. It does not show any impact on the computer or PC. It is used to build customers by giving the emails as results.

It is similar to the search engines, where you need to type any keyword related to the expected results. The same algorithm is designed here. If we want emails with a keyword which we want, we need to type in the search keyword section. The results are shown with the keyword included. Based on this, we can estimate our customers before itself and chose the keyword to search with relevancy. It is fully automated email finder, we just need to specify some

details related to the expected output, then we can get the expect email information data.

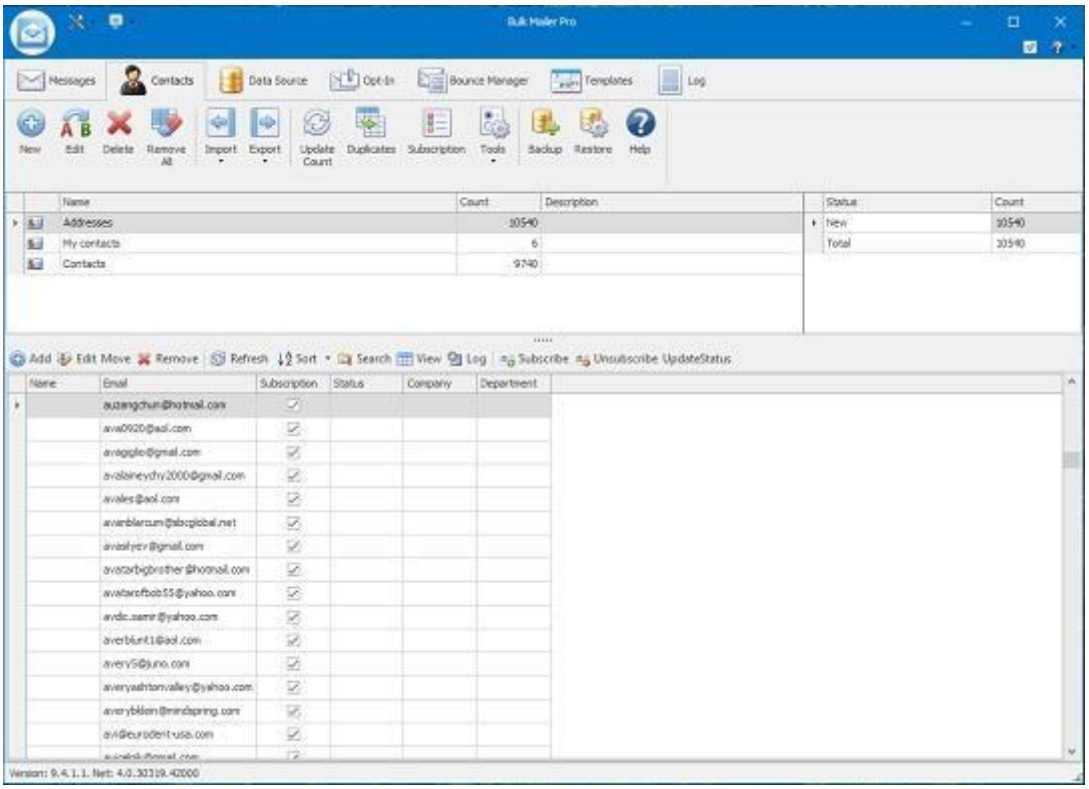


The Email Extractor pro gives the results in the way displayed above. It does the important and difficult task for you. It extracts the relevant emails for the key word from all of the internet. It is an advanced email extractor which searches the mails and extracts from major search engines like google, yahoo, Bing, etc. It also has an email verifier as shown below.



This email verifier verifies the emails whether they are correct, certain or uncertain ones.

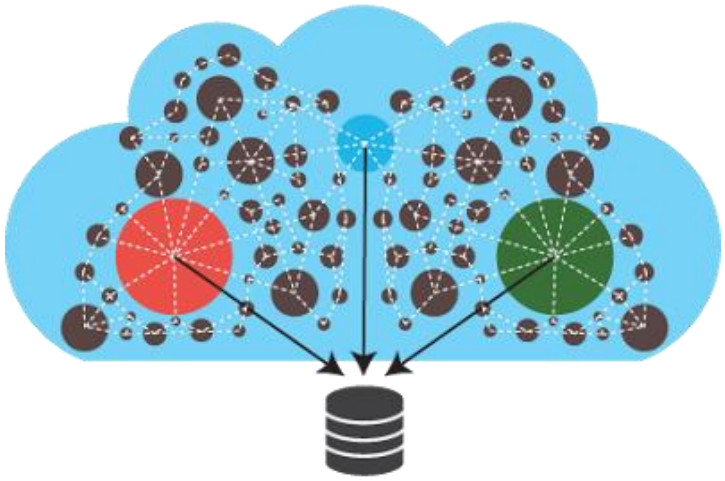
With the collecting and verifying of emails, the email extractor also helps in multi-email sending in a bulk amount like to all the emails collected at a time. These emails are collected to market the product of the person who is extracting the emails. He can just send the emails in a very vast number by just one click.



6) Web-Data Extractor:

The web data extractor is used to gather a large amount of data from the internet to our desired folders or viewing online. It is a tool which is only created and used for mass gathering of the different data types we require. The web data extractor can generate URLs, Emails, addresses, phone numbers, fax details, meta tags, etc. This is really a useful one which enables to gather information in a large content which is not at all illegal. We are just using the already available tools officially with the premium range. The web data extractor is a software that automatically and repeatedly extracts the data from web pages with matching the content with already taken data base and if there are any similar ones, it only sends a single copy of the data. It delivers all the extracted data to the database we already mentioned in the tool before going on with the process. It even shows which is the working data and which is uncertain data.

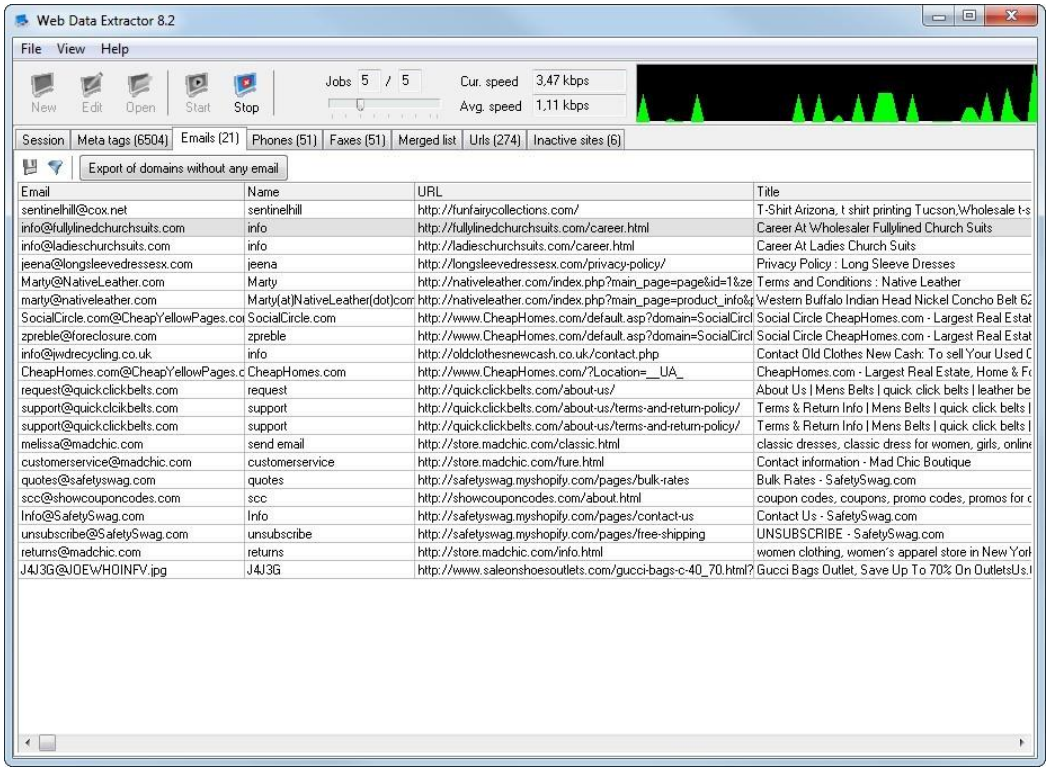
This web data extractor process is shown in the below diagram, accessing all the data from the internet by searching from all the known domains present on the internet relevant to the key word typed by the user.



The data can be exracted with all the information for the keyword like,

- Name.
- Email ID.
- URL.
- Title.
- Value
- Position. Etc.

The Web extractor algorithm is designed in way that the key word typed is being sent to the search engines which are connected by default to the extractor. There it checks with the search engines and websites matching with the relevant results of the keyword.



The above all are the tools and techniques used for information gathering.

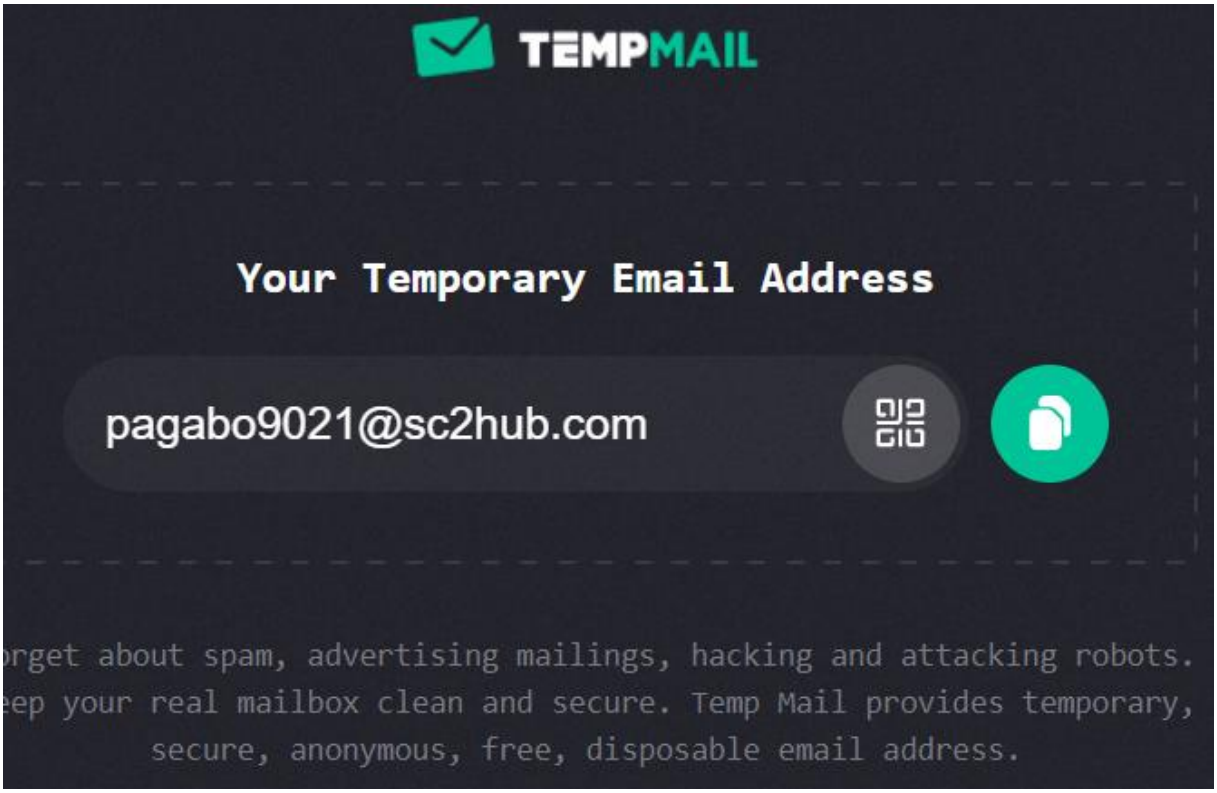
There are some tools which may be very useful while hacking or ethical hacking. They are shown below:

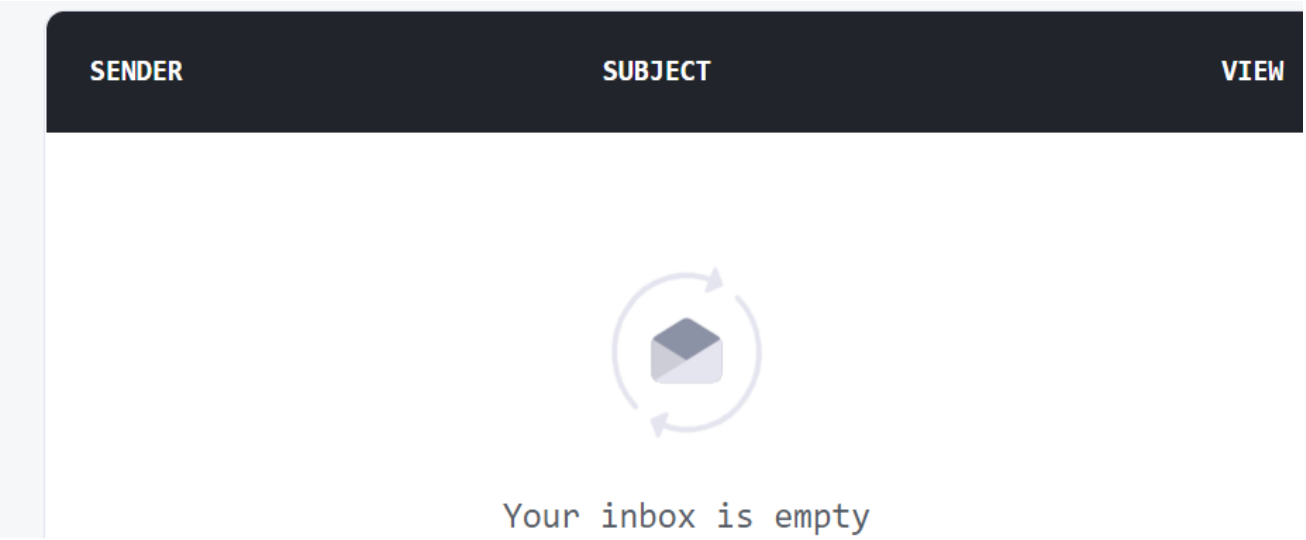
- YouGetSignal.
- Temp-mail.org.
- Temp Phone numbers to receive SMS
- Way back machine.

YouGetSignal: It is used to find the open ports in the IP address we give.

This is the website to use www.yougetsignal.com .

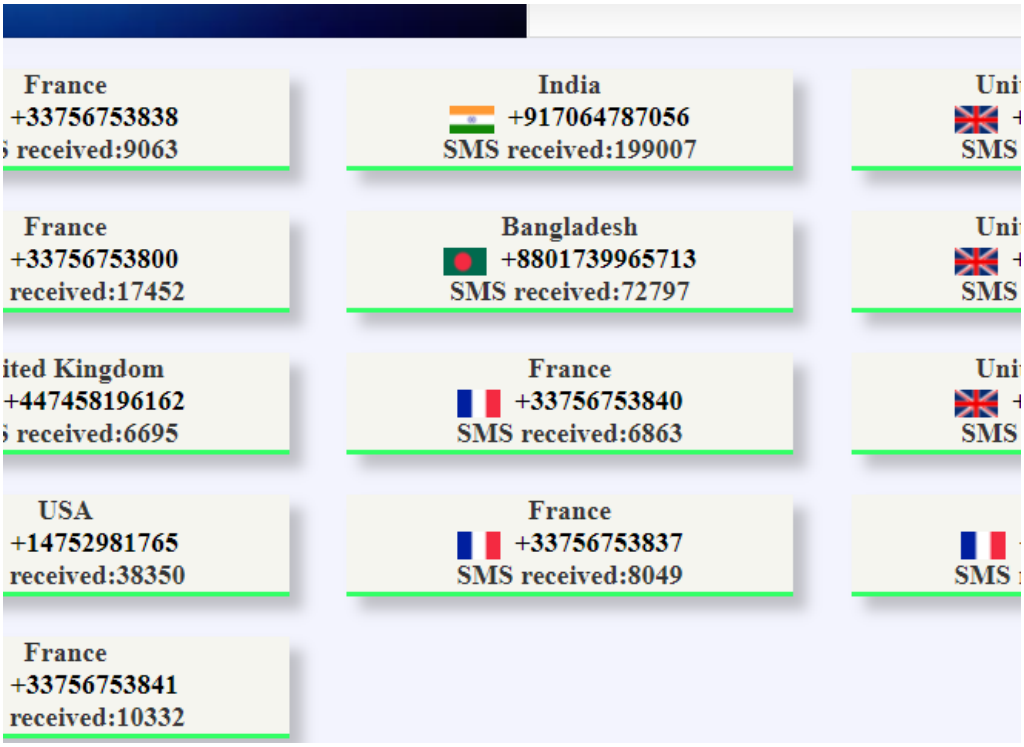
Temp-mail.org: It provides some temporary email addresses to the user to help him use this mail as his mail for the time being and even the inbox messages which is eve displayed in the site www.temp-mail.org .





It can be used to hide the original data of the user and use the utilities of a website with these mails. This is very useful when you don't know the consequences in any website to signup or login. The Hackers use this to hide their details and extract the data from the website they need as their target.

Receive SMS online: When we need to know the information, but we don't want to give our personal Contact, then we can use this website which provides some phone numbers of all countries which we can use for some time.

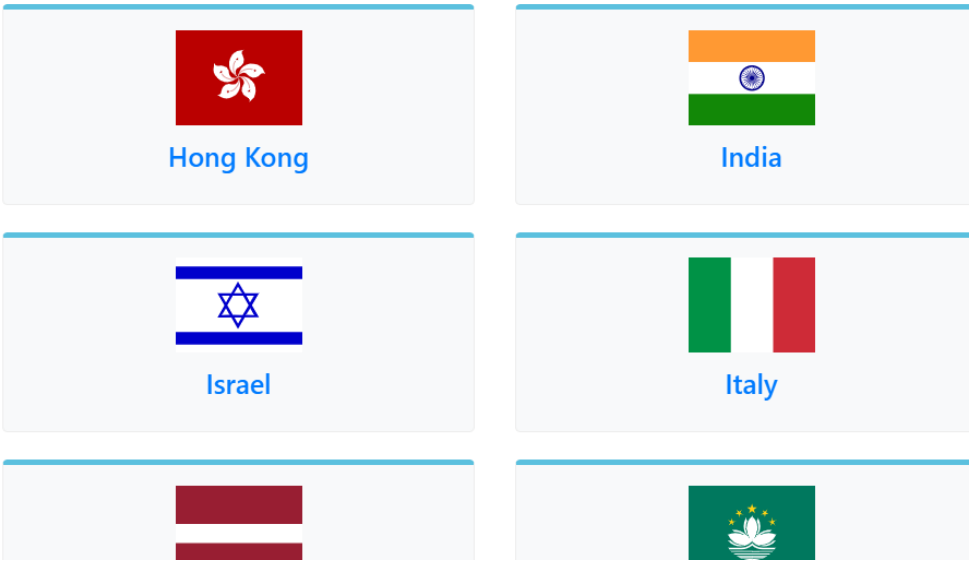


We even can receive messages on this number on which the messages are seen on the website itself under the specific portal. We can't receive phone calls here.

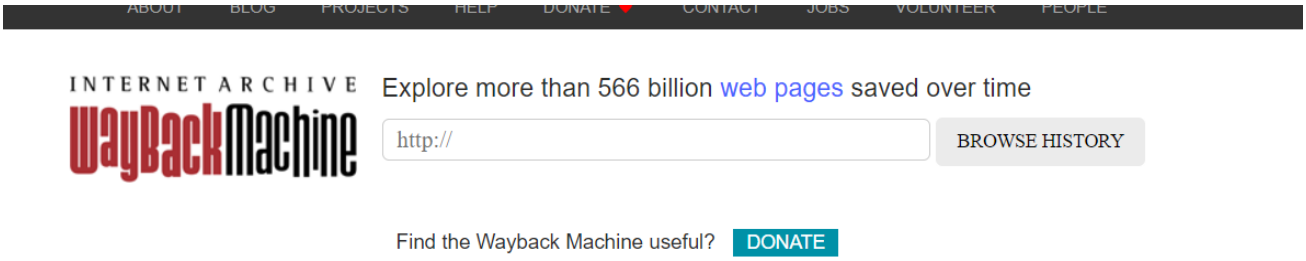
Website is www.receive-sms-online.info

K-BYJUIS	OTP for verification of mobile number for BNAT is 7463. This is valid for
P-UPSTOX	Your OTP for signing in on Upstox is 173341. The code will be valid for 5
M-XENDE	Your SMS verification code is:2289
M-HOTST	1037 is your Disney+ Hotstar verification code. Enjoy watching!
P-UPSTOX	Your OTP for signing in on Upstox is 639166. The code will be valid for 5
P-SCAPTL	your code is 6811
757XXXX	Doh, you already have a profile attached to this number and we currentl
M-Ncompl	Hello,Your verification code is 510258 . Don't share it with others.(NXCO

There are many other sites similar to these websites like www.sms24.com .

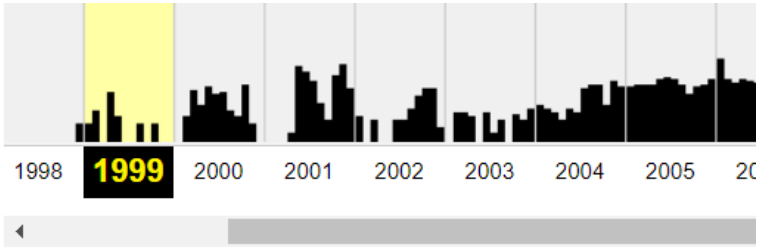


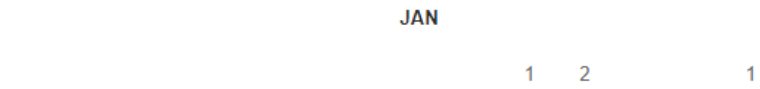
Way Back Machine: It is an online tool which shows the appearances of websites from its start date to till date. It takes us to the previous appearance of the website we want just like a time machine. It shows even the advertisements that were on the website that day. This is not really a usual one but an awesome one to find the website look from establishing to till the recent update. This can be used to find out the extension files added to that website. So that it would be easy for the attackers or testers to find the extension file and move according to that ones. We can only see the outer appearance but not the website process and response to the keys we give.



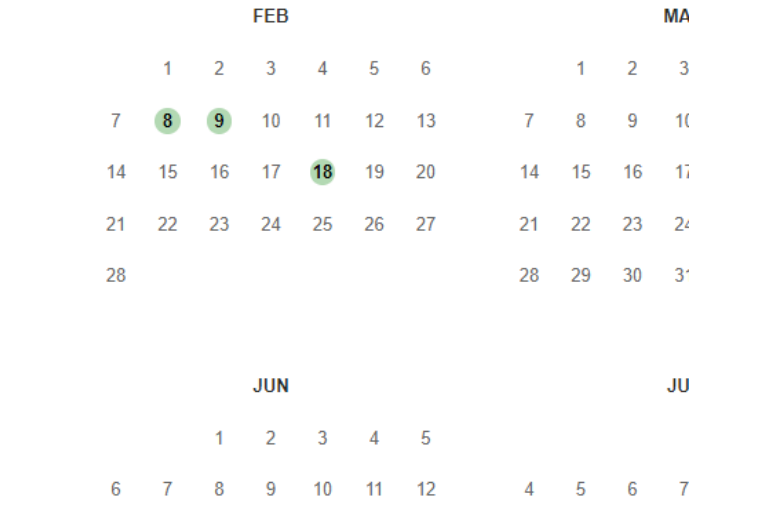
Here we can type the required URL in the specified box given and click the submit button. Then we can get the results

Let us take www.amazon.com in 1999 click on the year you want.





Now, click on the month you want.



We get the appearance of the site in that year.

☐ Here there some specific codes to be understood.
100- Processing.
200- ok.
300- Redirection.
400- Client-side errors.
500- Server-side errors.

☐ The bubbles in the way back machine shows.
200- Blue.
300- Green.
400- Orange.
500- Red.

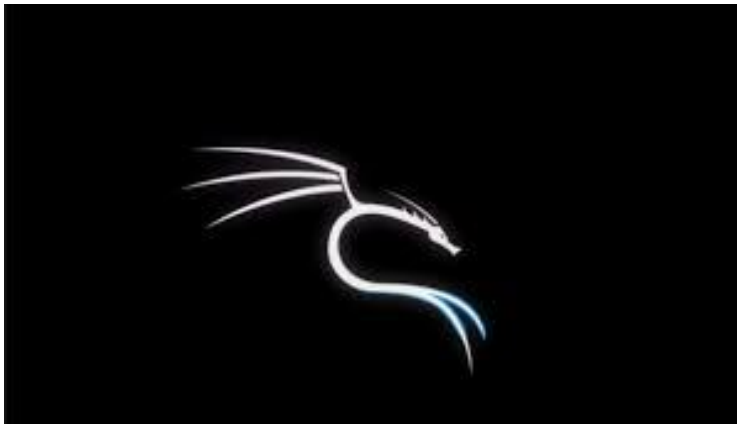
Important:

Now, let us know about "**KALI LINUX"**

There are many types of Linux in the market like kali, parrot security, backbox, Black Arch, Bugtraq, Deft Linux, etc. But most of the hackers, ethical hackers and penetration testers use "kali Linux" for better experience and very safe usage.

Kali Linux:

Kali Linux is a software which is comprised with a type of Linux operating system. The Kali Linux provides a very user-friendly environment and it is helpful for easy doing of the work of them. It is used for learning to hack and practicing penetration testing. Kali Linux is also a legal software or operating system. This is not illegal one. This is not only for penetration but also for security auditing of any system or website we want to know.



Why Kali Linux?

- It contains thousands of in-built hacking tools which are used for various security purposes and other like penetration testing, security research, Computer forensics and Reverse Engineering.

- It requires root account to use all these tools efficiently and effectively.
- It also allows us to gather information of any target or victim in large content compared to outer tools.
- It is very dangerous operating system when it is ought to defend. It is dangerous for the victim or target.
- It is very good OS even for beginners to learn an understand the processes.

 Install the latest Kali Linux software into the virtual box in the PC and then set up in the virtual box. This enables us to use the virtual box along with the windows OS already present in the PC originally.

Now, to open the required websites, use the link

Git clone- https://github.com/dbblackhat/admin-panel-finder.git in the Linux.

Networking:

The process of interacting with others and making relations with them to exchange the information and make business professionally or in any other format is called Networking. It is also the process of linking the networks, computers, computer systems, servers, etc. to work with interaction is called Networking. Here it allows sharing of data from one system to the other. Internet is an example of network which connect crores of other networks along with the servers, systems, computers and other electronic devices.

IP – Internet Protocol.

IP Address – The configuration of a computer/system is called IP address.

IPv4 – IPv4 is a 32bit binary numbered IP address. It is deployed in 1981. It contains 4.3 Billion addresses which must be reused and masked up. It follows manual protocol or DHCP (Dynamic Host Configuration Protocol). **Ex: 192.168.5.18**

IPv6: IPv6 is a 128bit alphanumeric hexadecimal numbered IP address. It contains 7.9*10^23 addresses. Every device has a unique address which is under IPv6. It supports the autoconfiguration. **Ex: 50b2:6400:0000:0000:6c3a:b17d:0000:10a9.**

In IP addresses, there are 2 types:

Public IP: It is the one which can be seen by everyone and it is registered IP. Like taking an account in a social media platform which can be accessed from any where we want.

Private IP: It is a personal IP which can't be accessed from other devices.

Classes of IP addresses:

Class A – 0 to 126. **127.0.0.1 -** Home

Class B – 128 to 191.

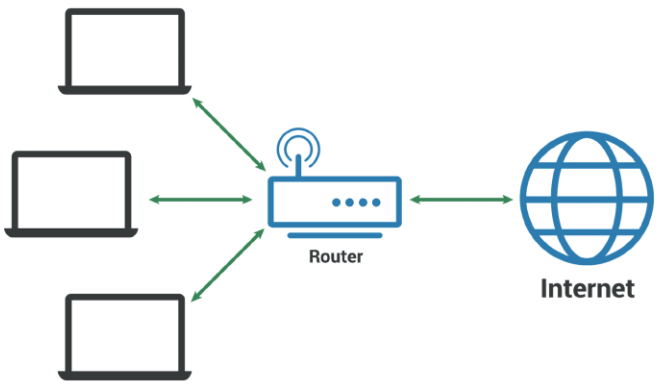
Class C- 192 to 223.

Class D – 224 to 239. (Multicast)

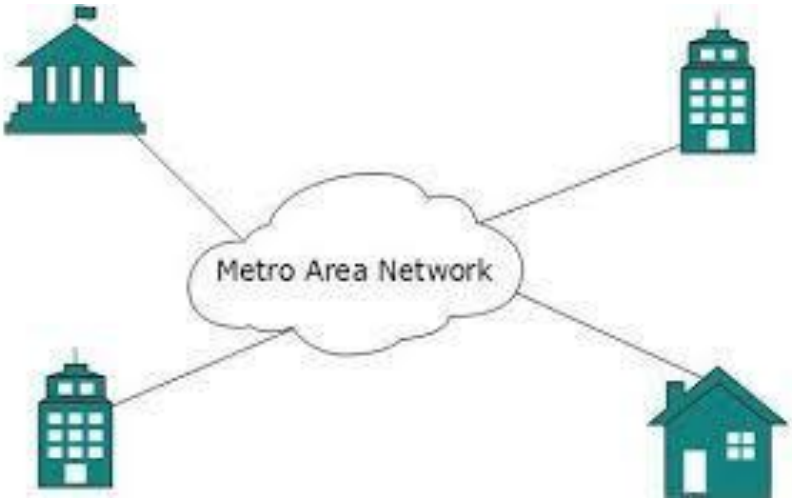
Class E – 240 to 255. (Reserved)

There are many types in the Networks:

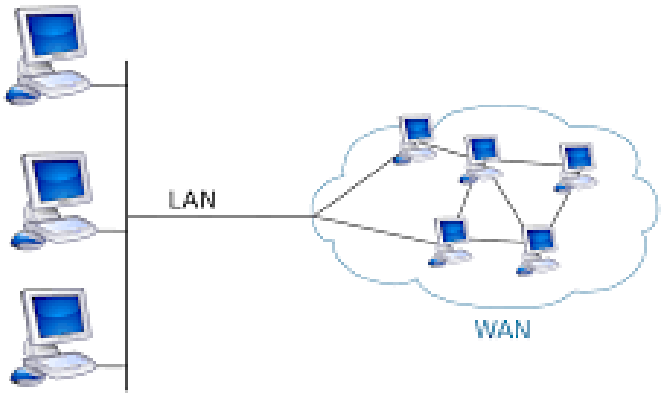
- **LAN –** Local Area Network.



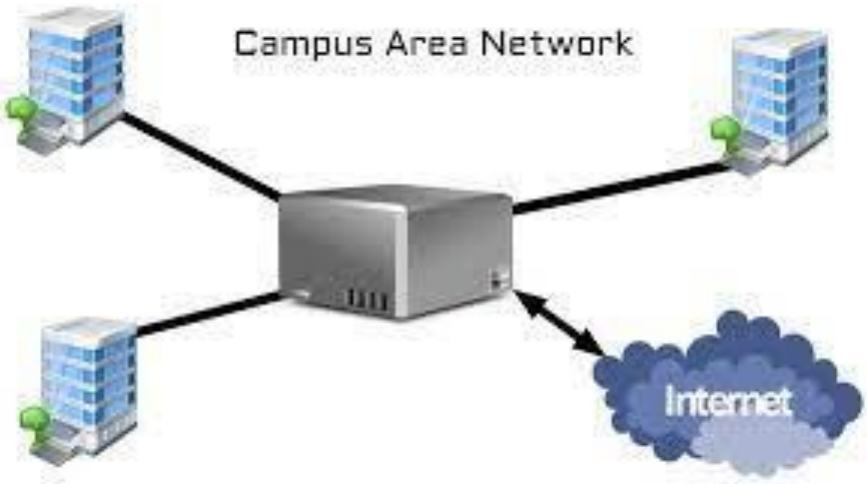
- **MAN –** Metropolitan Area Network.



- **WAN –** Wide Area Network.

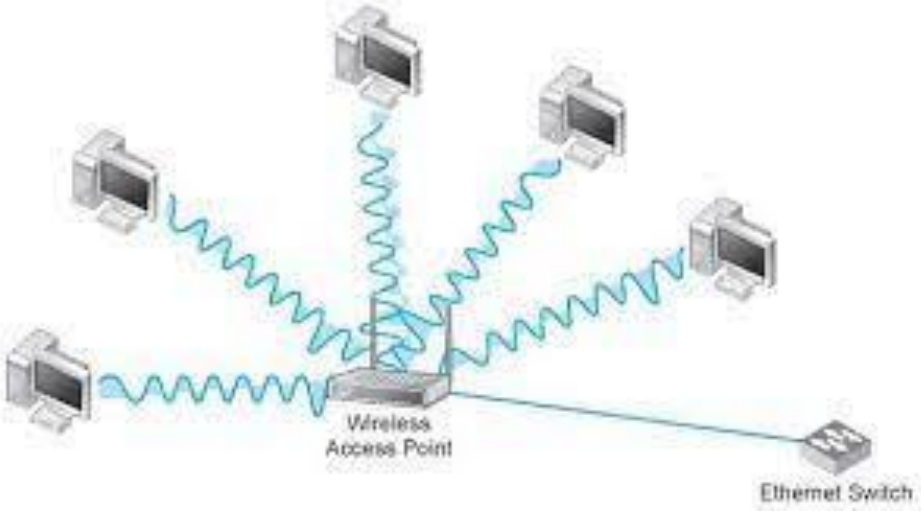


- **CAN –** Campus Area Network.

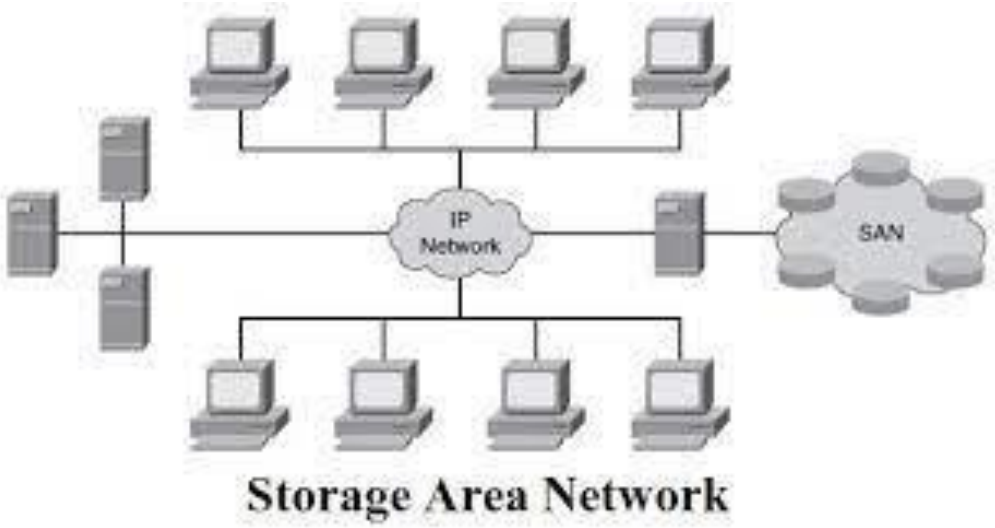


- **PAN –** Personal Area Network.

- **WLAN –** Wire Less Local Area Network.

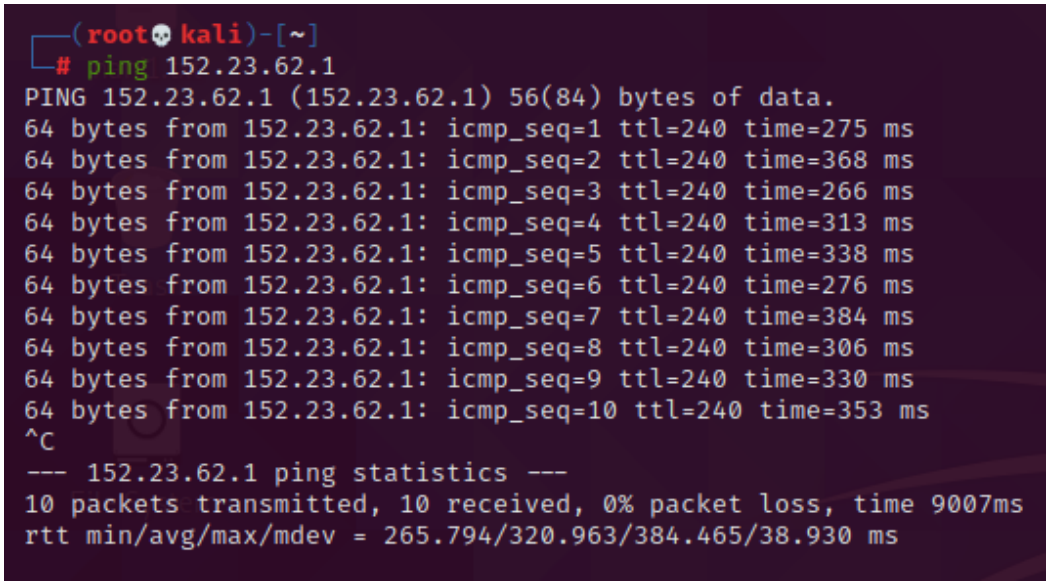


- **SAN –** Storage Area Network.



Activeness of the IP address can be determined with the command '**PING'.**

ping<space>IP address. (In the Linux terminal)



Enumeration:

It is the process of extracting all the information from a system like user names, machine names, network resources, shares, details of the users and services. The gathered information is used to identify the weak points, loop holes or vulnerabilities in the system's security and for exploiting the system for gaining the access to the server.

There are many methods for enumeration with different ports on different ports.

Port: The port is generally a communication end point. It is a logical opening in the software level which identifies the process and others like type of network service. Generally, there are approximately 65,535 ports. The ports start at UDP and ends with TCP there are 65,535 ports in between them.

- We most commonly come across ports like 80,443,20,21,22,23,25,53.

Port Number	Usage
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH)
23	Telnet - Remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail Routing
53	Domain Name System (DNS) service
80	Hypertext Transfer Protocol (HTTP) used in World Wide Web

110	Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of Digital Mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

The following are the few networking ports:

Enumeration using Nmap Script engine:

ftp enumeration:

- **nmap –script ftp-anon -p 21:**
  1. nmap –script ftp-anon www.sjctni.edu :

```
┌──(root💀kali)-[~]
└─# nmap --script ftp-anon www.sjctni.edu
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-24 07:29 EST
Nmap scan report for www.sjctni.edu (210.212.250.34)
Host is up (0.036s latency).
Other addresses for www.sjctni.edu (not scanned): 64:ff9b::d2d4:fa22
rDNS record for 210.212.250.34: sjctni.edu
Not shown: 990 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   open   ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Mar 23  2017 pub
22/tcp   open   ssh
53/tcp   open   domain
80/tcp   open   http
443/tcp  open   https
445/tcp  open   microsoft-ds
8082/tcp closed blackice-alerts
8085/tcp open   unknown
8093/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 53.61 seconds
```

  2. nmap –script ftp-anon www.stannscollegehyd.com :

```
┌──(root💀kali)-[~]
└─# nmap --script ftp-anon www.stannscollegehyd.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-24 07:33 EST
Nmap scan report for www.stannscollegehyd.com (103.53.43.177)
Host is up (0.019s latency).
Other addresses for www.stannscollegehyd.com (not scanned): 64:ff9b::6735:2bb1
Not shown: 853 filtered ports, 132 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
25/tcp   open  smtp
26/tcp   open  rsftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 71.87 seconds
```

3. nmap –script ftp-anon ftp.mirror.nl :

```
┌──(root💀kali)-[~]
└─# nmap --script ftp-anon ftp.mirror.nl
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-24 07:46 EST
Nmap scan report for ftp.mirror.nl (194.109.21.67)
Host is up (0.0033s latency).
Other addresses for ftp.mirror.nl (not scanned): 2001:888:0:25::43
rDNS record for 194.109.21.67: dl.xs4all.nl
Not shown: 980 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| lrwxrwxrwx    1 0        0              19 Jan 18  2006 debian → ./pub/mirror/debian
| drwxr-xr-x   13 0        0            4096 Jan 29  2020 pub
|_-rw-r--r--    1 0        0              26 Mar 04  2010 robots.txt
80/tcp   open   http
443/tcp  open   https
3000/tcp closed ppp
49154/tcp closed unknown
49156/tcp closed unknown
49175/tcp closed unknown
49400/tcp closed compaqdiag
50002/tcp closed iiimsf
50500/tcp closed unknown
50800/tcp closed unknown
52673/tcp closed unknown
52869/tcp closed unknown
54045/tcp closed unknown
56737/tcp closed unknown
58080/tcp closed unknown
60443/tcp closed unknown
64680/tcp closed unknown
65000/tcp closed unknown
65129/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 130.07 seconds
```

4. nmap –script ftp-anon [ftp.iij.ad.jp](ftp.iij.ad.jp) :

```
┌──(root💀kali)-[~]
└─# nmap --script ftp-anon ftp.iij.ad.jp
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-24 11:43 EST
Nmap scan report for ftp.iij.ad.jp (202.232.140.10)
Host is up (0.12s latency).
Other addresses for ftp.iij.ad.jp (not scanned): 2001:240:bb8f:f::10
rDNS record for 202.232.140.10: nas1800.ftp.pub.2iij.net
Not shown: 990 closed ports
PORT    STATE    SERVICE
21/tcp  open     ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x   18 ftp      ftp           320 Oct 13 16:10 pub
25/tcp  open     smtp
53/tcp  open     domain
80/tcp  open     http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     https
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
873/tcp open     rsync

Nmap done: 1 IP address (1 host up) scanned in 15.16 seconds
```

5. nmap –script ftp-anon ftp.gwdg.de :

```
┌──(root💀kali)-[~]
└─# nmap --script ftp-anon ftp.gwdg.de
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-24 11:47 EST
Nmap scan report for ftp.gwdg.de (134.76.12.6)
Host is up (0.16s latency).
Other addresses for ftp.gwdg.de (not scanned): 2001:638:60f:110::1:2
rDNS record for 134.76.12.6: ftp6.gwdg.de
Not shown: 991 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x   59 ftp      ftp          4096 Jan 24 13:32 pub
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
443/tcp   open   https
873/tcp   open   rsync
30000/tcp closed ndmps
30718/tcp closed unknown
30951/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 17.63 seconds
```

http enumeration:

nmap –script http-enum.nse -p 80 www.example.com

- **nmap –script http-drupal-enum-users.nse -p 80:**
  1. nmap –script http-drupal-enum-users.nse -p 80 www.shape.com :

```
┌──(root💀kali)-[~]
└─# nmap --script http-drupal-enum-users.nse -p 80 www.shape.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 14:16 EST
Nmap scan report for www.shape.com (13.33.93.76)
Host is up (0.029s latency).
Other addresses for www.shape.com (not scanned): 13.33.93.85 13.33.93.28 13.33.93.124
rDNS record for 13.33.93.76: server-13-33-93-76.mrs52.r.cloudfront.net

PORT   STATE SERVICE
80/tcp open  http
| http-drupal-enum-users:
|   a-hjelvik
|   a-navy
|   A+Stewart
|   A+Gough+75
|   a-hjelvi
|   a-junghansweb
|   a.armbrust
|   a-trice
|   a-mpadilla9610832
|   a-lhoffman@hotmail.com
|   b-lenius
|   b-email
|   b-anikahotmail
|   b-delgado
|   b-nissen
|   b-nelson
|   b+illmcsgirl
|   b-anders
|   b-jenglish
|   b+bess
|   c-a_edwards
|   c-storage
|   c-byrd
|   c-dickinsonsbc
|   c-thurber
|   c.barker
|   C.Ashbacher
|   c.baumgarth
|   c-miller46508
|   c-dodge
|   d-ricks
|   d-harrell2011
|   D&#039;Etta
|   d-knees
|   d-fasickhotmai
|   d-tkane1
|   d-kearns
|   d-schutt
|   d-bate6287773
|   d-n3rd
|   e-luong
```

  2. nmap –script http-drupal-enum-users.nse -p 80 www.seobook.com :

```
┌──(root💀kali)-[~]
└─# nmap --script http-drupal-enum-users.nse -p 80 www.seobook.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-24 12:10 EST
Nmap scan report for www.seobook.com (45.79.65.120)
Host is up (0.28s latency).
rDNS record for 45.79.65.120: rock.seobook.com

PORT   STATE SERVICE
80/tcp open  http
| http-drupal-enum-users:
|   A Katie Lunn Creation
|   a rahim
|   A Love Bug
|   A Personal Square
|   A Kumar
|   A Beautiful Mind 4
|   a
|   A Plus Insurance
|   A Happy Dog Supplies
|   A Lenny Locksmith in Tampa
|   b-jou
|   b
|   b-real09
|   b-green
|   B-marketer
|   b-webs
|   b.k.
|   B.
|   b.cunningham
|   b.allen
|   C-Bas
|   C
|   C Bloom
|   C. Bowens
|   C Phillips
|   c.labra
```

- **nmap –script http-drupal-enum.nse -p 80:**
  1. nmap –script http-drupal-enum.nse -p 80 www.shape.com

```
┌──(root💀kali)-[~]
└─# nmap --script http-drupal-enum.nse -p 80 www.shape.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 14:21 EST
Nmap scan report for www.shape.com (13.33.93.124)
Host is up (0.029s latency).
Other addresses for www.shape.com (not scanned): 13.33.93.28 13.33.93.76 13.33.93.85
rDNS record for 13.33.93.124: server-13-33-93-124.mrs52.r.cloudfront.net

PORT   STATE SERVICE
80/tcp open  http
| http-drupal-enum:
|   Themes:
|     omega
|_    aurora

Nmap done: 1 IP address (1 host up) scanned in 117.53 seconds
```

  2. nmap –script http-drupal-enum.nse -p 80 www.seobook.com :

```
┌──(root💀kali)-[~]
└─# nmap --script http-drupal-enum.nse -p 80 www.seobook.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-24 13:00 EST
Nmap scan report for www.seobook.com (45.79.65.120)
Host is up (0.26s latency).
Other addresses for www.seobook.com (not scanned): 2600:3c01::f03c:91ff:fe3b:f4ff
rDNS record for 45.79.65.120: rock.seobook.com

PORT   STATE SERVICE
80/tcp open  http
| http-drupal-enum:
|   Modules:
|     views
|     token
|     ctools
|     pathauto
|     libraries
|     entity
|     date
|     link
|     webform
|     backup_migrate
|     google_analytics
|     devel
|     views_bulk_operations
|     globalredirect
|     email
|     page_title
|     redirect
|     mailsystem
|     auto_nodetitle
|     cck
|     mimemail
|     simplenews
|_    logintoboggan

Nmap done: 1 IP address (1 host up) scanned in 8.91 seconds
```

- **nmap--script http-wordpress-enum.nse -p 80:**
  1. nmap--script http-wordpress-enum.nse -p 80 nrtec.in:

```
┌──(root💀kali)-[~]
└─# nmap --script http-wordpress-enum.nse www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 14:32 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0081s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
| http-wordpress-enum:
| Search limited to top 100 themes/plugins
|   plugins
|     akismet
|     contact-form-7
|     wordpress-seo
|     wordpress-importer
|     mailchimp-for-wp
|     wp-smushit
|     broken-link-checker
|     redirection
|     wp-mail-smtp
|   themes
|     twentyfifteen 2.8
|     twentysixteen 2.3
|_    twentyseventeen 2.5

Nmap done: 1 IP address (1 host up) scanned in 80.37 seconds
```

  2. nmap--script http-wordpress-enum.nse -p 80 nrtec.in:

```
┌──(root💀kali)-[~]
└─# nmap --script http-wordpress-enum.nse www.smce.ac.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-24 13:24 EST
Nmap scan report for www.smce.ac.in (103.21.58.130)
Host is up (0.039s latency).
rDNS record for 103.21.58.130: bh-in-5.webhostbox.net
Not shown: 980 closed ports
PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  open     ssh
25/tcp  open     smtp
26/tcp  open     rsftp
53/tcp  open     domain
80/tcp  open     http
| http-wordpress-enum:
| Search limited to top 100 themes/plugins
|   plugins
|     contact-form-7
|     si-contact-form
|     contact-form-plugin
|     contact-bank
|   themes
|     twentyfifteen 1.9
|     twentysixteen 1.6
|_    twentyseventeen 1.8
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
| http-wordpress-enum:
| Search limited to top 100 themes/plugins
|   plugins
|     contact-form-7
|     si-contact-form
|     contact-form-plugin
|     contact-bank
```

- **nmap –script http-wordpress-users.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script http-wordpress-users.nse www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 15:00 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0085s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
| http-wordpress-users:
| Username found: administrator
| Username found: suneel
| Username found: savya
| Username found: susmith
| Username found: kishore
| Username found: swapnil
| Username found: bhavani
| Username found: nagrik
| Username found: rishib
| Username found: maineditor
|_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-users.limit'

Nmap done: 1 IP address (1 host up) scanned in 23.02 seconds
```

- **nmap –script http-userdir-enum.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script http-userdir-enum.nse www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 14:37 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0097s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
|_http-userdir-enum: Potential Users: guest, web, test

Nmap done: 1 IP address (1 host up) scanned in 8.11 seconds
```

- **nmap --script http-enum.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script http-enum.nse -p 80 www.kitsguntur.ac.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 14:46 EST
Nmap scan report for www.kitsguntur.ac.in (45.35.47.173)
Host is up (0.00095s latency).
rDNS record for 45.35.47.173: skugexams.in

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

- **nmap –script http -robots.txt.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script http-robots.txt.nse www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 14:51 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0083s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
| http-robots.txt: 2 disallowed entries
|_/wp-admin/ /latest-updates/

Nmap done: 1 IP address (1 host up) scanned in 5.33 seconds
```

- **nmap –script http -passwd.nse:**

Passwords can't be found that easy for any websites. It can't be easily found for any website.

```
┌──(root💀kali)-[~]
└─# nmap --script http-passwd.nse www.shape.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:10 EST
Nmap scan report for www.shape.com (13.33.93.28)
Host is up (0.065s latency).
Other addresses for www.shape.com (not scanned): 13.33.93.124 13.33.93.85 13.33.93.76
rDNS record for 13.33.93.28: server-13-33-93-28.mrs52.r.cloudfront.net
Not shown: 996 filtered ports
PORT    STATE  SERVICE
25/tcp  closed smtp
53/tcp  open   domain
80/tcp  open   http
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 53.45 seconds
```

smb enumeration:

- **nmap –script smb-os-discovery.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script smb-os-discovery.nse -p 445 www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:06 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.00092s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

- **nmap –script smb-enum shares.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script smb-enum-shares.nse -p 445 www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:08 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0016s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds

┌──(root💀kali)-[~]
└─# nmap --script smb-enum-shares.nse -p 445 www.shape.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:08 EST
Nmap scan report for www.shape.com (13.33.93.124)
Host is up (0.00090s latency).
Other addresses for www.shape.com (not scanned): 13.33.93.76 13.33.93.85 13.33.93.28
rDNS record for 13.33.93.124: server-13-33-93-124.mrs52.r.cloudfront.net

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
```

smtp enumeration:

- **nmap –script smtp-enum-users.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script smtp-enum-users.nse www.smosh.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:13 EST
Nmap scan report for www.smosh.com (23.227.38.74)
Host is up (0.014s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
| smtp-enum-users:
|_  Couldn't establish connection on port 25
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 37.24 seconds
```

ssl enumeration:

- **nmap –script ssl-cert.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script ssl-cert.nse www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:23 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0085s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
| ssl-cert: Subject: commonName=www.nrtec.in
| Subject Alternative Name: DNS:nrtec.in, DNS:www.nrtec.in
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-11-20T09:42:45
| Not valid after:  2021-02-18T09:42:45
| MD5:   6e8f e26c 2538 3922 c303 f8d4 74d9 2f55
|_SHA-1: 6f6b b3d0 6b03 1b1c e7ef fabb 8c69 33f1 669a 3f4e

Nmap done: 1 IP address (1 host up) scanned in 21.03 seconds
```

- **nmap –script ssl-enum-ciphers.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script ssl-enum-ciphers.nse www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:27 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0079s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       Key exchange (ecdh_x25519) of lower strength than certificate key
|_  least strength: A

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

- **nmap –script ssl-date.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script ssl-date.nse www.amreddyengineering.ac.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:31 EST
Nmap scan report for www.amreddyengineering.ac.in (194.59.164.164)
Host is up (0.079s latency).
Not shown: 921 filtered ports
PORT    STATE SERVICE
21/tcp    open  ftp
|_ssl-date: TLS randomness does not represent time
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
|_ssl-date: 2021-01-24T04:45:38+00:00; +13m52s from scanner time.
1023/tcp  open  netvenuechat
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1028/tcp  open  unknown
1038/tcp  open  mtqp
1061/tcp  open  kiosk
1065/tcp  open  syscomlan
1082/tcp  open  amt-esd-prot
1095/tcp  open  nicelink
1104/tcp  open  xrl
1112/tcp  open  msql
1152/tcp  open  winpoplanmess
1154/tcp  open  resacommunity
1233/tcp  open  univ-appserver
1277/tcp  open  miva-mqs
1301/tcp  open  ci3-software-1
1434/tcp  open  ms-sql-m
1580/tcp  open  tn-tl-r1
1687/tcp  open  nsjtp-ctrl
1720/tcp  open  h323q931
1801/tcp  open  msmq
2000/tcp  open  cisco-sccp
2008/tcp  open  conf
2013/tcp  open  raid-am
2021/tcp  open  servexec
2033/tcp  open  glogger
```

dns enumeration:

- **nmap –script dns-blacklist.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script dns-blacklist.nse -p 53  www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:37 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0059s latency).

PORT   STATE SERVICE
53/tcp open  domain

Host script results:
| dns-blacklist:
|   SPAM
|_    bl.spamcop.net - FAIL

Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
```

- **nmap –script dns-service-discovery.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script dns-service-discovery.nse -p 53  www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:40 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0032s latency).

PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds
```

tls enumeration:

- **nmap –script tls-alpn.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script tls-alpn.nse -p 443 www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:42 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0044s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

- **nmap –script tls-nextprotoneg.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script tls-nextprotoneg.nse -p 443 www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:43 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0042s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
```

telnet enumeration:

- **nmap –script telnet-encryption.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script telnet-encryption.nse -p 23 www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:46 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.00095s latency).

PORT   STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds
```

- **nmap –script telnet-ntlm-info.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script telnet-ntlm-info.nse -p 23 www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:48 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0011s latency).

PORT   STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

mysql enumeration:

- **nmap –script mysql-databases.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script mysql-databases.nse -p 3306 www.nrtec.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:50 EST
Nmap scan report for www.nrtec.in (167.71.231.97)
Host is up (0.0016s latency).

PORT     STATE    SERVICE
3306/tcp filtered mysql

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

- **nmap –script mysql-enum.nse:**

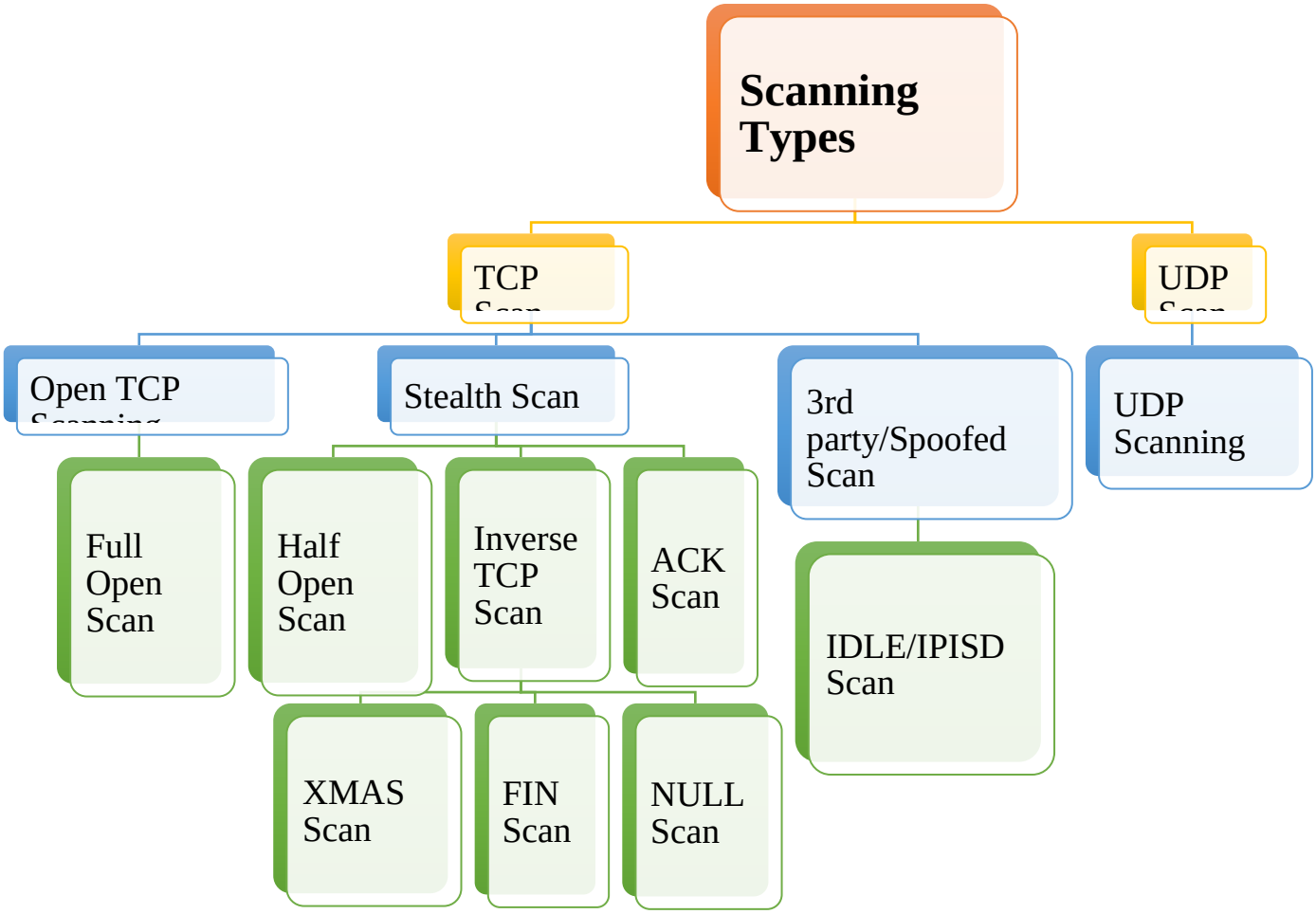
```
┌──(root💀kali)-[~]
└─# nmap --script mysql-enum.nse -p 3306 www.amreddyengineering.ac.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:53 EST
Nmap scan report for www.amreddyengineering.ac.in (194.59.164.164)
Host is up (0.0071s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-enum:
|   Valid usernames:
|     admin:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     root:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

- **nmap –script mysql-info.nse:**

```
┌──(root💀kali)-[~]
└─# nmap --script mysql-info.nse -p 3306 www.amreddyengineering.ac.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 23:55 EST
Nmap scan report for www.amreddyengineering.ac.in (194.59.164.164)
Host is up (0.0070s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.4.14-MariaDB-cll-lve
|   Thread ID: 525942150
|   Capabilities flags: 63486
|   Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, Support41Auth, Speaks41ProtocolOld, D
tsTransactions, SupportsLoadDataLocal, FoundRows, IgnoreSigpipes, SupportsAuthPlugins, SupportsMu
|   Status: Autocommit
|   Salt: X\G+AFyQi>9Ay`Tbr6T$
|_  Auth Plugin Name: mysql_native_password

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```

Scanning: It is set of methods which are used in finding the live hosts, ports, services, finding the OS and model of the victim's system or

computer. It also identifies vulnerabilities and threats in the network connected to the system. It comprises of using critical and aggressive reconnaissance/Information Gathering techniques.

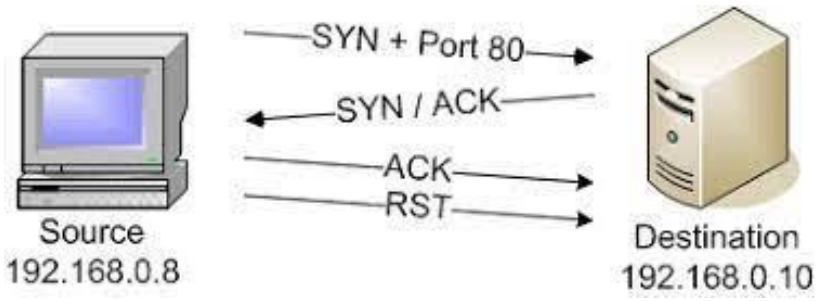


UDP Scan: UDP Scan is different from TCP Scan. It does not need existing network connections. The network systems use UDP scan for broad casting messages. One to many sending port, much like unsolicited junk emails. The most common UDP packets – DNS registrations and name resolution queries are sent to port 53.

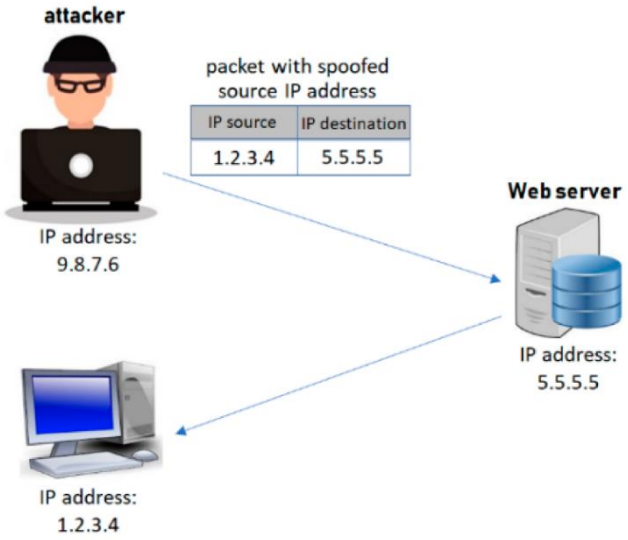
TCP Scan: TCP Scan is commonly involving a full connection for transferring data and then eventually reducing it. This involves sending a large number of packets of

data to every port that is scanned until then. Compared to all the types of scanning, it is slow and done with a procedure systematically.

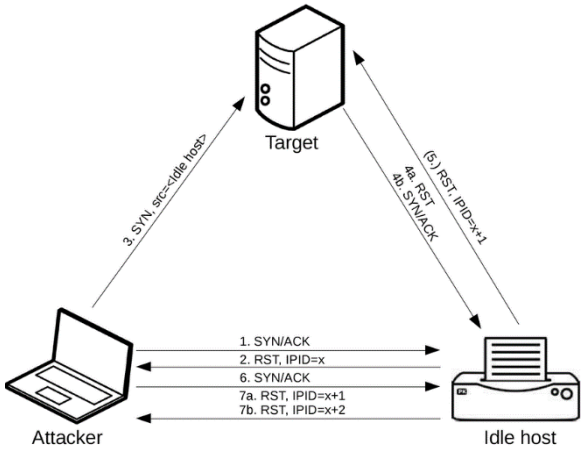
- **Full Open Scan:**



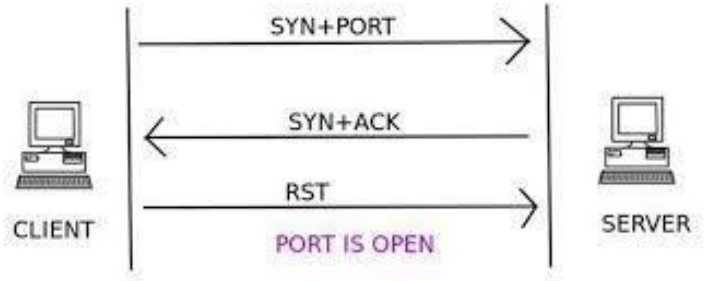
Third Party/Spoofed Scan:



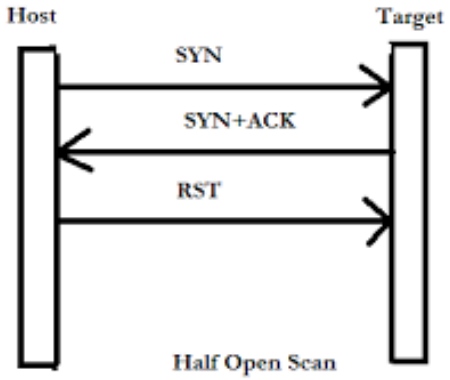
IDLE Scan: It is a method of scanning that involves sending spoofed packets to a computer to find the services which are available.

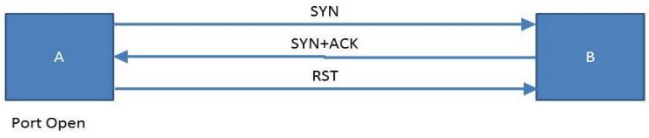


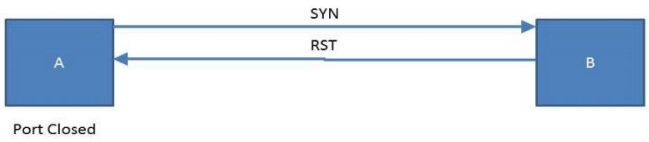
Stealth Scan: We get the accurate results on the stealth scan.



Half Open Scan: It is a default scanner. Once it got response, it sets the port to reset.



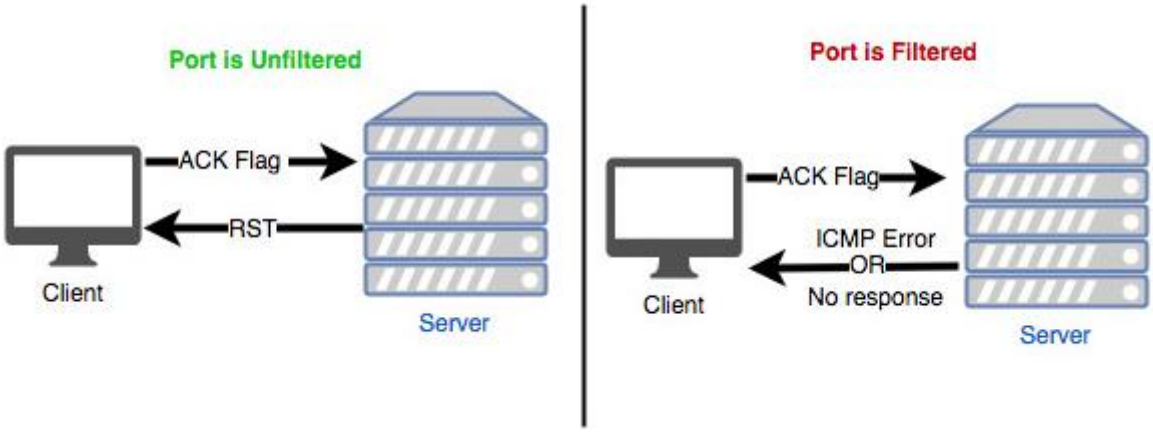




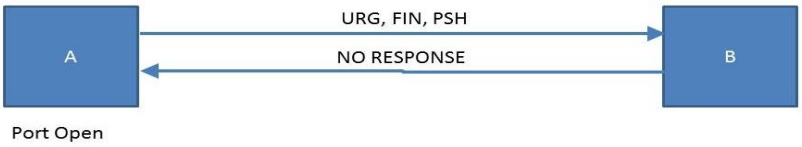
Inverse TCP Scan: It is sending the TCP packets without TCP flags. Based on the response it gets, decision is taken whether it is closed or open. If there is no response the port is open. If there is any response, the port is reset.

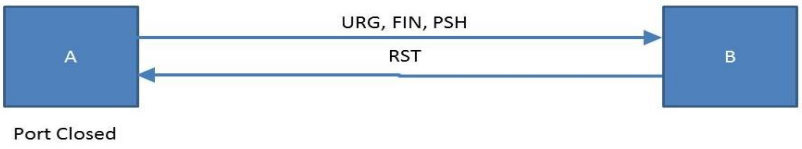
Inverse TCP Flag Probe Scanning

ACK Scan: It does not work on the windows operating system. In nmap is specified and enabled by **'-sA'.** The ACK Scan never determines whether the ports are open or not. They are used to determine whether there are firewalls and the ports which are filtered out.

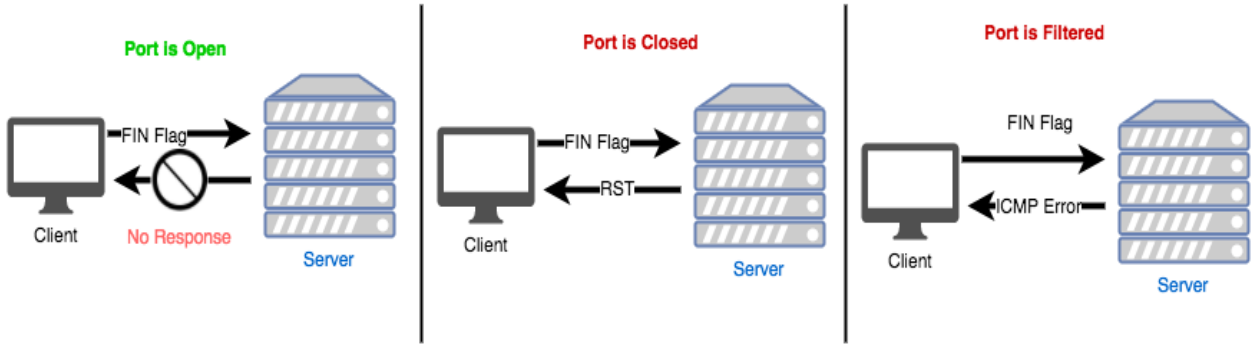


XMAS Scan: This scan is designed to manipulate the PSH, URG and FIN flags of the TCP header.

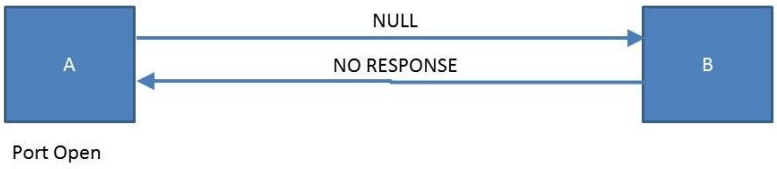




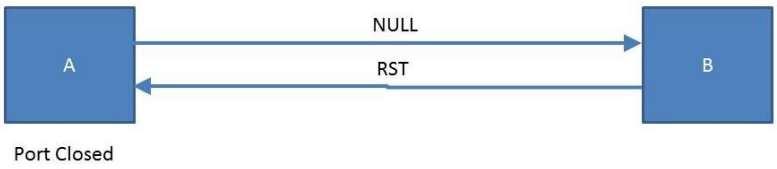
FIN Scan: FIN Scan sends packet of data which is not existed until then. It sends the packets with FIN flag set in it without establishing a connection with the target. If no packet is received, the port is open and if a reset packet is received, the port is open.



NULL Scan: If the TCP Scan is sent with no flag, it is considered as NULL Scan.



Port Open



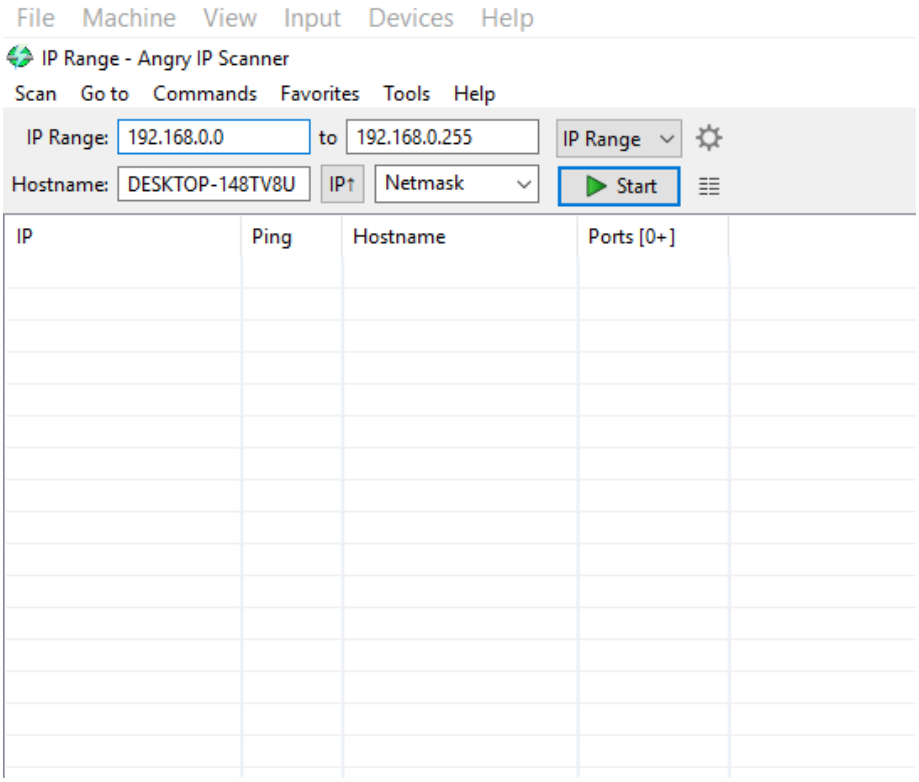
Port Closed

Scanning Tools:

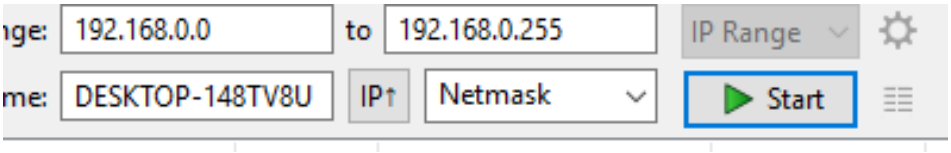
There are many scanning tools to do the process of scanning. Some of them are given here:

1) **Angry IP Scanner:**
   The Angry IP Scanner is used to ping vast number of multiple IP addresses at a time. It can scan the IP addresses in a large number at any range and even can scan the ports of the specific addresses and gives the results with the status of the IP addresses and their ports.

   The IP addresses are being scanned in this application in the range we set them. It firstly pings each IP address and checks whether the IP is active or not. If its is alive, then its further pings the hostnames, address, scan ports, etc. It is frequently used by both black and white hat hackers. Because, it helps to find the weakness in a device.



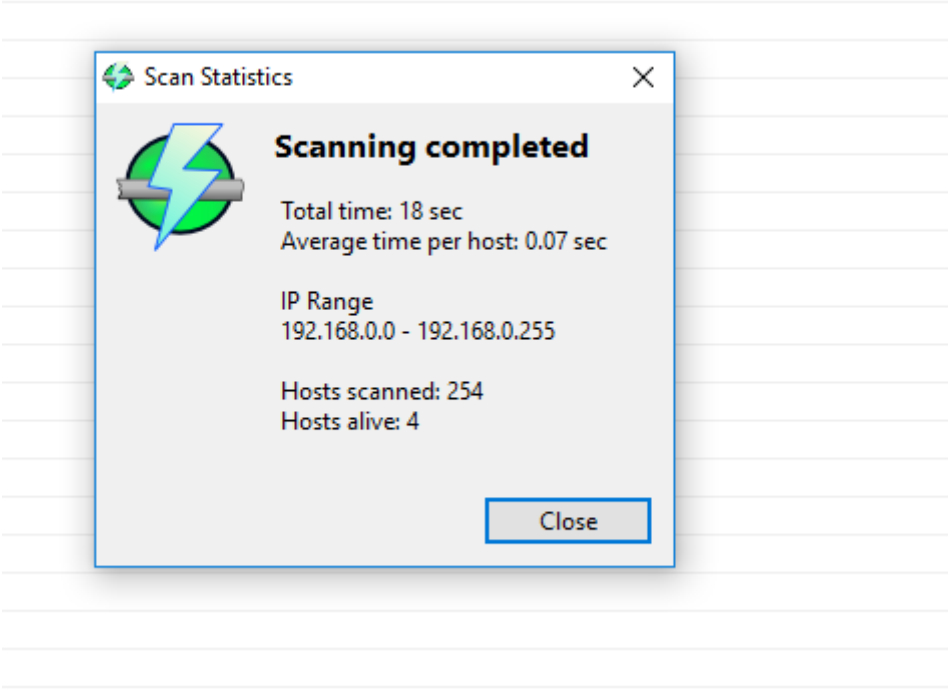
The Angry IP scanner looks like this. This has a domain to note down the IP address range we want to know the active status.



The IP addresses range is set and the stat button is enabled, then with the process going on we can know the hostnames and IP also for every device.

192.168.0.97	[n/a]	[n/s]	[n/s]
192.168.0.98	[n/a]	[n/s]	[n/s]
192.168.0.99	[n/a]	[n/s]	[n/s]
192.168.0.100	[n/a]	[n/s]	[n/s]
192.168.0.101	1 ms	Android.local	[n/s]
192.168.0.102	286 ms	[n/a]	[n/s]
192.168.0.103	[n/a]	[n/s]	[n/s]
192.168.0.104	[n/a]	[n/s]	[n/s]
192.168.0.105	[n/a]	[n/s]	[n/s]
192.168.0.106	[n/a]	[n/s]	[n/s]
192.168.0.107	[n/a]	[n/s]	[n/s]
192.168.0.108	0 ms	DESKTOP-148TV8U	[n/s]
192.168.0.109	[n/a]	[n/s]	[n/s]
192.168.0.110	[n/a]	[n/s]	[n/s]
192.168.0.111	[n/a]	[n/s]	[n/s]
192.168.0.112	[n/a]	[n/s]	[n/s]
192.168.0.113	[n/a]	[n/s]	[n/s]
192.168.0.114	[n/a]	[n/s]	[n/s]

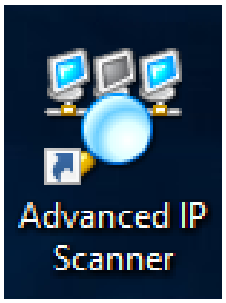
It shows the active stats of the Ip addresses it pinged in the range given. And shows the alive IPs in blue colour and inactive IPs in red colour.



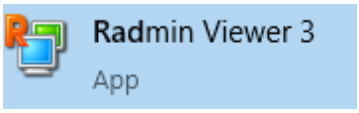
Once the scan is completed it shows the total number of hosts scanned and which are alive. The time taken to scan is also shown. There is dialogue box displayed as shown in the figure.

2) Advanced IP Scanner:

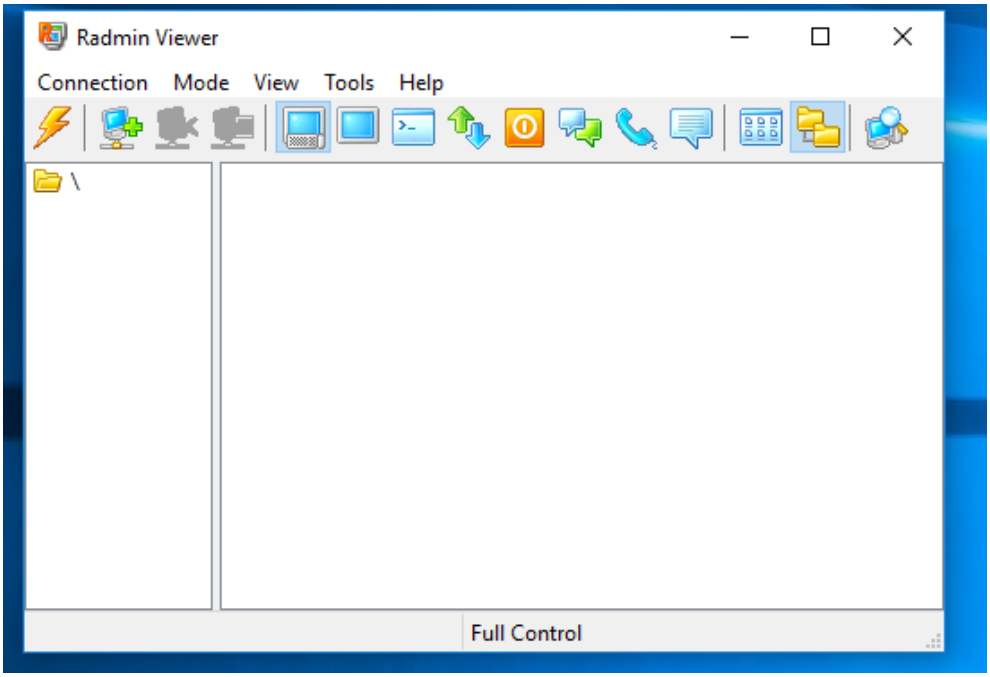
Angry IP Scanner is the fastest and free tool for the network scanning. It enables us to detect all the computers in the network and give access to them if they are vulnerable. If fond any computers or systems vulnerable, then we can just control the computer with just a single click. Turing it ON and OFF.



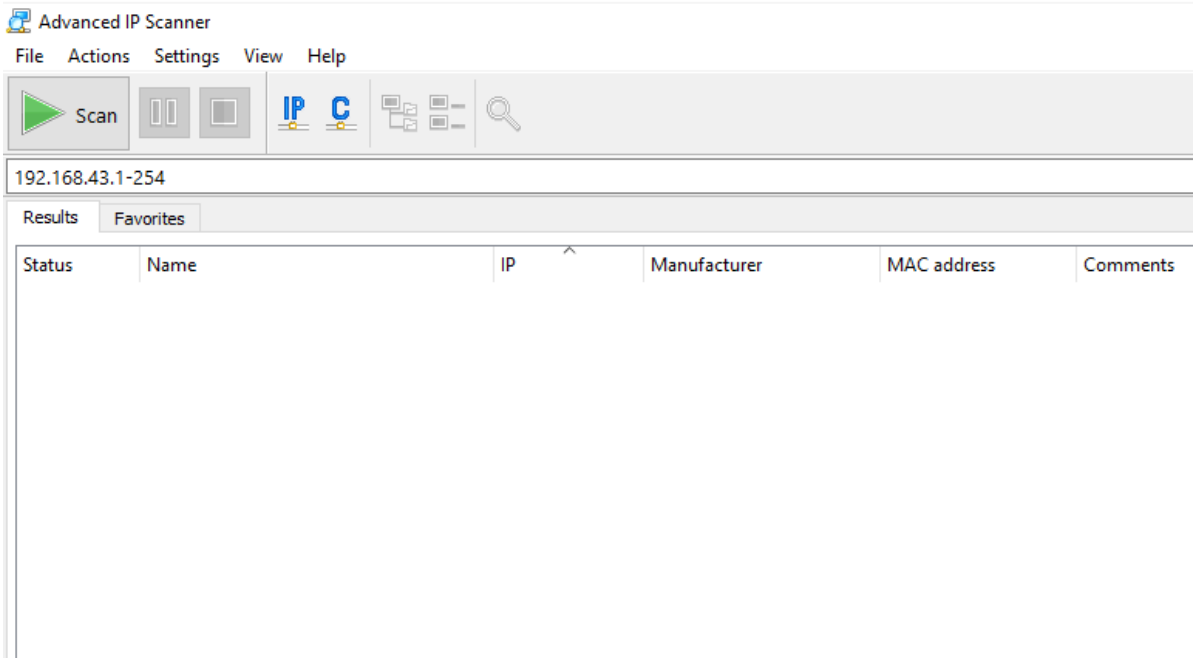
To do this, we need to connect the advanced IP scanner to the Radmin server. The Radmin sever is a quite complex one with the security standards of the Microsoft windows firewall and security. While using these, the firewall and the security must be turned off.



When we use the Radmin server by opening it, we can see a dialogue box as shown here.

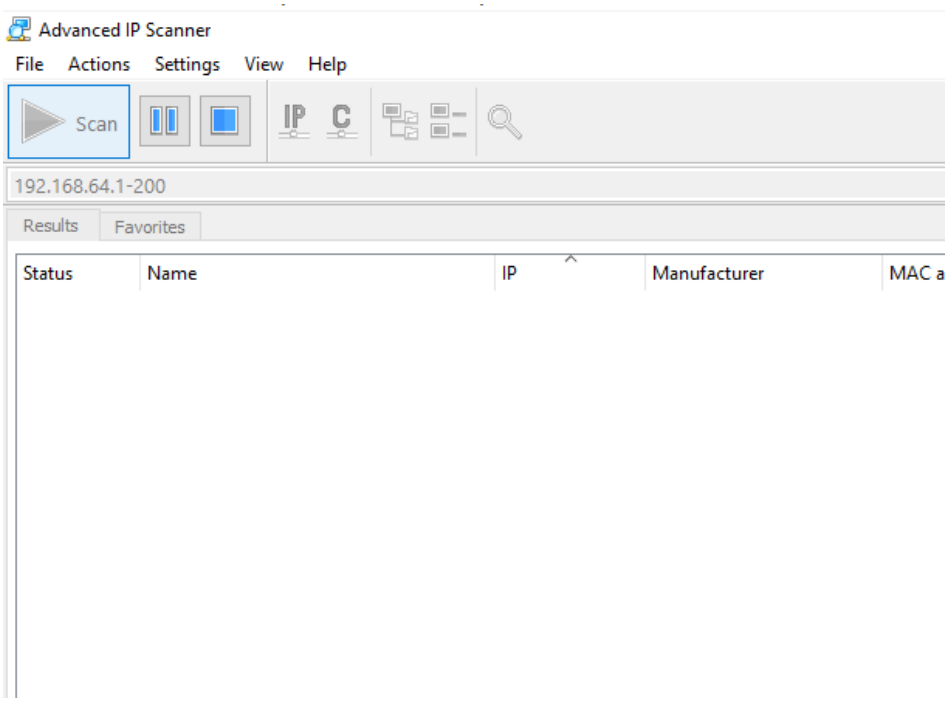


The advanced IP scanner enables us to scan the vulnerable and active computers in the network as shown.



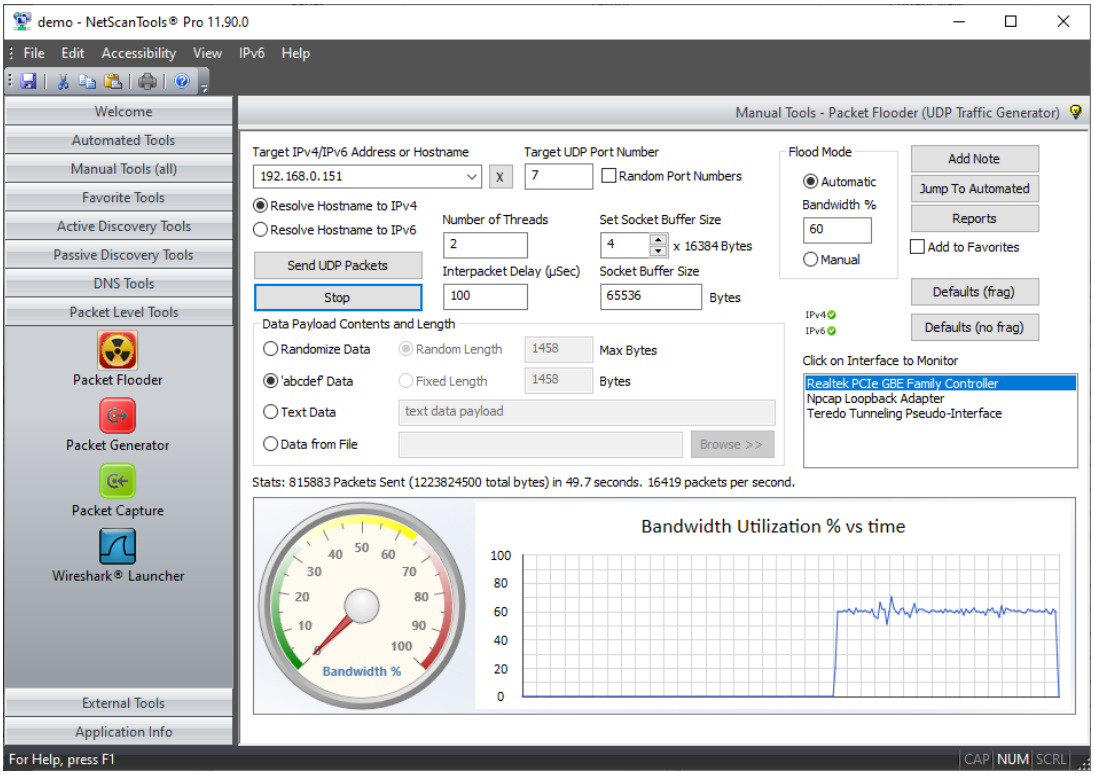
There is a domain to enter the IP addresses range when opened the app.

We can just enter the range of IP addresses we need and click the scan button. Then the scanning starts, if there are any active computer systems or vulnerable ones, then it displays the address of it in the dialogue box



3) Net Scan Tools Pro:

The Net Scan Tools Pro comprises of the collection of internet information gathering and network vulnerabilities detecting algorithm for the usage of the network professionals and high-end hackers or ethical hackers. It is used to research IPv4 and IPv6 addresses, host names, email addresses, URLs, automatically within the process itself.



The Net scan tool pro is used for this type of scanning. This is widely use by the Network professionals.

```
┌──(root💀kali)-[~]
└─# chmod +r nani1.py

┌──(root💀kali)-[~]
└─# ls -l
total 68
drwxr-xr-x 3 root root 4096 Jan  9 09:21 admin-panel-finder
drwxr-xr-x 3 root root 4096 Feb  1 09:49 Cam-Hackers
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Desktop
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Documents
drwxr-xr-x 2 root root 4096 Feb  5 08:46 Downloads
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Music
-rw-r--r-- 1 root root    0 May 17 13:51 nani1
-rw------- 1 root root    2 May 17 14:24 nani12345.py.save
-rw-rw-rw- 1 root root   96 May 17 14:16 nani1.py
-rw-r--r-- 1 root root    5 Jan 10 06:24 nanibujji
-rw-r--r-- 1 root root  105 Jan 10 06:22 nanibujji.txt
-rw-r--r-- 1 root root   35 May 17 14:07 nanisagar.txt
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Pictures
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Public
-rw-r--r-- 1 root root    0 May 17 13:50 sagar
drwxr-xr-x 5 root root 4096 Feb  1 09:48 ShellPhish
drwxr-xr-x 6 root root 4096 Jan 13 09:17 sherlock
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Templates
drwxr-xr-x 2 root root 4096 Jan  9 08:22 Videos
```