# INDEX

Q1.Install and configure any Antivirus software on System .

Ans 1

# Antivirus

Antivirus is the data security software which provides extremely advanced protection from unknown viruses, spywares, malware, worms, Trojans and other internet threats. Antivirus doesn’t just provide protection from unknown threats but also features like firewall , Email Protection (Scanning incoming & outgoing mails and block specific files in outgoing attachments).

**There are two ways antivirus software will be delivered to you:**

- You will be getting a package of CD, product key and instruction manual
- Or you will get the product key and instruction manual online and a link to download the antivirus software.

**Before installing antivirus software, you should check the following things:**

- Make sure that no other virus protection solutions are installed.
- The automatic protection functions of various security solutions may interfere with each other.
- You should have an established internet connection.

**Now it’s time to get into the steps which needs to be followed while installing antivirus software:**

1. Install by running the setup with “antivirusname.exe” installation file by double clicking over it.
2. After that a pop screen will appear and ask for user account authorization, you need to click on “Yes” which will take you to Antivirus setup screen.
3. Click “Next” and the installation Wizard will then guide you through the rest of the installation process.
4. Thereafter, a license agreement screen will appear where you will be asked to read about the minimum system requirements and then confirm that you to agree to the end-user license conditions.
5. To continue, the user need to select “I accept the agreement” which will activate the “Next” button for further steps.
6. Then the user needs to click on “Next” to reach destination selection window.
7. In the destination selection window, you will be asked to confirm the destination directory where the antivirus is going to get installed. The setup is designed in such a way that it selects the destination automatically or will create the same if doesn’t exist. It is recommended that you should accept the default destination directory and only need to click on “Next” to continue.
8. It will take you to the “Select Start Menu folder” Window to place the program’s shortcuts. By default it will store in the “Antivirus Name” folder, otherwise you can browse a different location. Click on “Next” to continue.
9. Now the user needs to select a server as Primary Update Definitions Server from a drop down list. We recommend that you should accept the default selected server and click on “Next” to continue.
10. Now the setup is ready to install the antivirus software. You need to click on “Install” to start the installation process.
11. Thereafter, you will see installation progress in the form of green progression bar. After the green bar is completed, the installation progress is successfully completed and ensures you with the “Finish” setup wizard.

12. As you click on “Finish” to complete the process, the installation part is completed. Now it’s time to register the antivirus product as it will be showing as demo installation having an expiry period of 30 days (the day might differ).
13. To register the antivirus product, you need to click on license and fill out necessary details like first name, last name, company (if any), phone number (optional), email address, country.
14. There after you need to enter the product serial key which you have got either in the box delivered to you or got it from online portal.
15. After entering the serial key, you just need to click on OK and message will be displayed “You products has been registered”

Note: We recommend restarting the system after installing antivirus software in order to get the registry updated and work fine without any issues.

Q2. Implement prevention mechanisms to protect PC from Cyber Attack .
Ans 2. Prevention mechanisms to protect PC from Cyber Attacks are:

- ✓ **Use a firewall**

  Firewalls prevent unauthorized access to your business network and alert you to any intrusion attempts.

  Make sure the firewall is enabled before you go online. You can also purchase a hardware firewall from companies such as Cisco, Sophos or Fortinet, depending on your broadband router, which also has a built-in firewall that protects your network. If you have a larger business, you can purchase an additional business networking firewall.

- ✓ **Install antivirus software**

  Antivirus software plays a major role in protecting your system by detecting real-time threats to ensure your data is safe. Some advanced antivirus programs provide automatic updates, further protecting your machine from the new viruses that emerge every day. After you install an antivirus program, don't forget to use it. Run or schedule regular virus scans to keep your computer virus-free.

  Antivirus programs such as Bitdefender, Panda Free Antivirus, Malwarebytes and Avast protect your computer against unauthorized code or software that may threaten your operating system.

- ✓ **Install an anti-spyware package**

  Spyware is a special kind of software that secretly monitors and collects personal or organizational information. It is designed to be hard to detect and difficult to remove and tends to deliver unwanted ads or search results that are intended to direct you to certain (often malicious) websites.

- ✓ **Use complex passwords.**

  Using secure passwords is the most important way to prevent network intrusions. The more secure your passwords are, the harder it is for a hacker to invade your system.

  More secure often means longer and more complex. Use a password that has at least eight characters and a combination of numbers, uppercase and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes.Don't use recognizable words or combinations that represent birthdays or other information that can be connected to you.

- ✓ **Keep your OS, apps and browser up-to-date**

  Always install new updates to your operating systems. Most updates include security fixes that prevent hackers from accessing and exploiting your data. The same goes for apps. Today's web browsers are increasingly sophisticated, especially in privacy and security. Be sure to review your browser security settings in addition to installing all new updates. For example, you can use your browser to prevent websites from tracking your movements, which increases your online privacy. Or, use one of these private web browsers.

- ✓ **Use two-factor authentication**

  Passwords are the first line of defense against computer hackers, but a second layer boosts protection. Many sites let you enable two-factor authentication, which boosts security because it requires you to type in a numerical code – sent to your phone or email address – in addition to your password when logging in.

### ✓ Back up your computer

If your business is not already backing up your hard drive, you should begin doing so immediately. Backing up your information is critical in case hackers do succeed in getting through and trashing your system.

Always be sure you can rebuild as quickly as possible after suffering any data breach or loss. Backup utilities built into macOS (Time Machine) and Windows (File History) are good places to start. An external backup hard drive can also provide enough space for these utilities to operate properly.

### ✓ Ignore spam

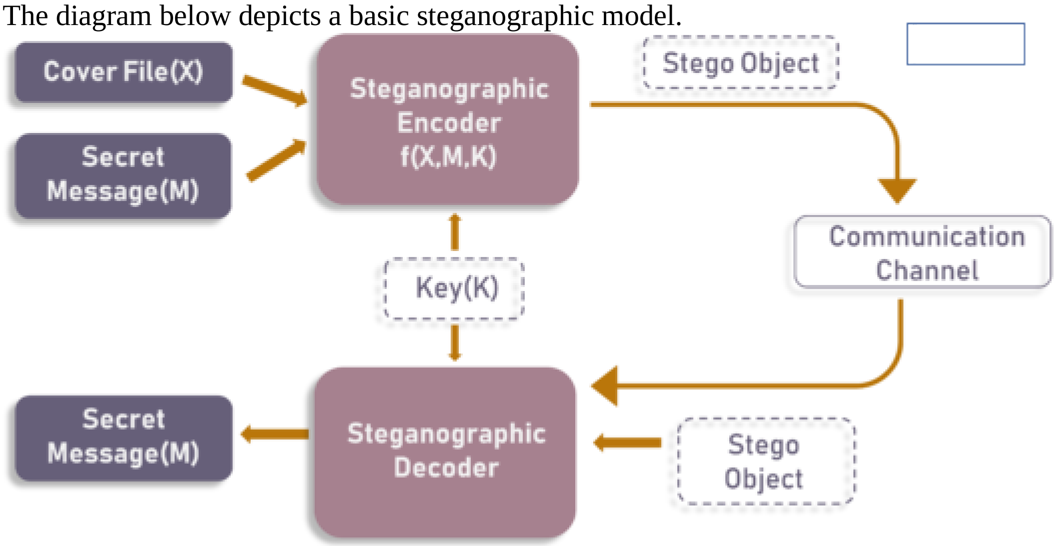
Beware of email messages from unknown parties, and never click on links or open attachments that accompany them. Inbox spam filters have gotten pretty good at catching the most conspicuous spam. But more sophisticated phishing emails that mimic your friends, associates and trusted businesses (like your bank) have become common, so keep your eyes open for anything that looks or sounds suspicious.

Q3.Implement Steganography Algorithms

Ans 3

**Steganography** is the art and science of embedding secret messages in a cover message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.

The diagram below depicts a basic steganographic model.



As the image depicts, both cover file(X) and secret message(M) are fed into steganographic encoder as input. Steganographic Encoder function, f(X,M,K) embeds the secret message into a cover file. Resulting Stego Object looks very similar to your cover file, with no visible changes. This completes encoding. To retrieve the secret message, Stego Object is fed into Steganographic Decoder.

**Depending on the nature of the cover object (actual object in which secret data is embedded), steganography can be divided into five types:**

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

Q4.Implement and install the keyloggers to understand their working.
Ans 4

**Keyloggers** or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Keyloggers are a form of spyware where users are unaware their actions are being tracked. Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. Some keyloggers can also capture your screen at random intervals; these are known as screen recorders. Keylogger software typically stores your keystrokes in a small file, which is either accessed later or automatically emailed to the person monitoring your actions.

## How Does a Keylogger Get on Your Computer?

A keylogger can be installed on your computer any number of ways. Anyone with access to your computer could install it; keyloggers could come as a component part of a virus or from any application installation, despite how deceptively innocent it may look. This is part of the reason why you should always be sure you're downloading files from a trusted resource.

## Keylogger Software

Remote- access software keyloggers can allow access to locally recorded data from a remote location. This communication can happen by using one of the following methods:

- Uploading the data to a website, database or FTP server.
- Periodically emailing data to a predefined email address.
- Wirelessly transmitting data through an attached hardware system.
- Software enabling remote login to your local machine.

Additional features that some software keyloggers come with can capture additional information without requiring any keyboard key presses as input. They include:

- Clipboard logging – Anything that can be copied to the clipboard is captured.
- Screen logging – Randomly timed screenshots of your computer screen are logged.
- Control text capture – The Windows API allows for programs to request the text value of some controls, meaning that your password may be captured even if behind a password mask (the asterisks you see when you type your password into a form).
- Activity tracking – Recording of which folders, programs and windows are opened and also possibly screenshots of each.
- Recording of search engine queries, instant message conversations, FTP downloads along with any other internet activities.

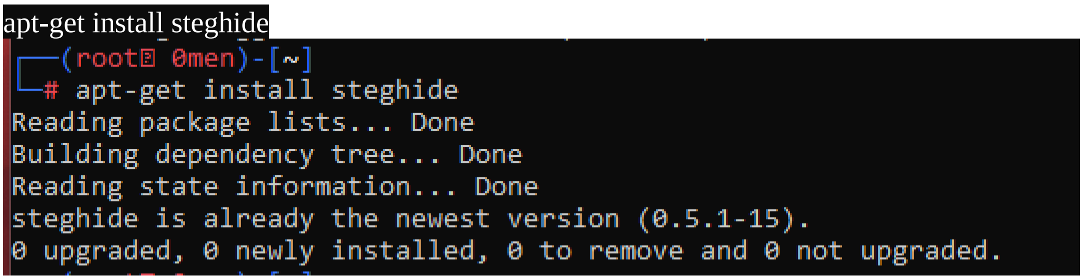
Q5.Implement hiding of Data in image using tools.
Ans 5. Hiding of Data in image is known as Image Steganangraphy.

Linux users can choose from a variety of open-source tools such as Steghide, Exif, Stegosuite, Steg, Outguess, and many more.

1. **Steghide**: Is an open-source, command-line software that can encode and decode data into image files.

**Installation**: Steghide is already available in the Kali Linux repo.

```
apt-get install steghide
```



```
┌──(root㉿0men)-[~]
└─# apt-get install steghide
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
steghide is already the newest version (0.5.1-15).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

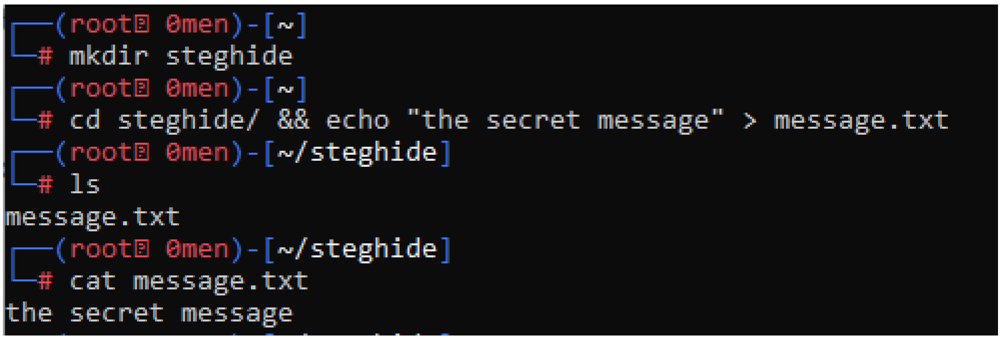
**<u>Creating an image with a secret message in it.</u>**

- Create a folder with the name of your choice:

```
mkdir steghide
```

- Create a new text files with some text. – This will be the secret that we want to embed in the image of our choice.

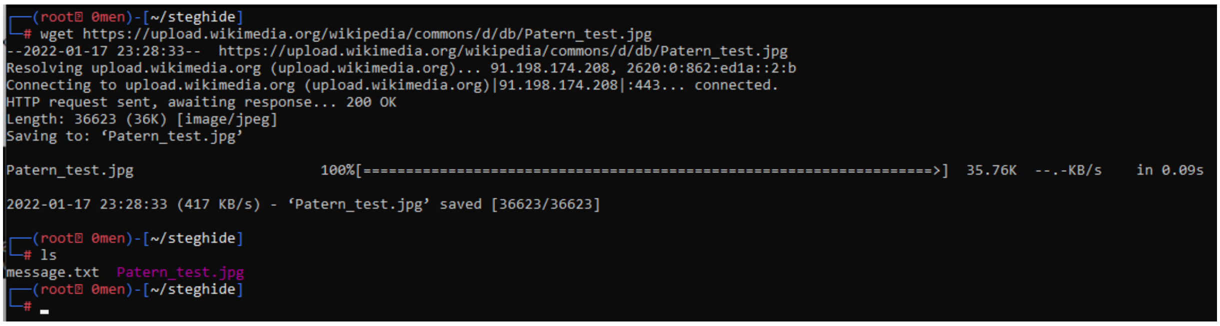
```
cd steghide
echo "the secret message" > message.txt
```



```
┌──(root㉿0men)-[~]
└─# mkdir steghide
┌──(root㉿0men)-[~]
└─# cd steghide/ && echo "the secret message" > message.txt
┌──(root㉿0men)-[~/steghide]
└─# ls
message.txt
┌──(root㉿0men)-[~/steghide]
└─# cat message.txt
the secret message
```

- **Download or use an image of your choice to hide the secret message.**

For this example we used his test image that you can download it using wget <image link>, and experiment on it, or you can choose your own.



```
┌──(root㉿ 0men)-[~/steghide]
└─# wget https://upload.wikimedia.org/wikipedia/commons/d/db/Patern_test.jpg
--2022-01-17 23:28:33--  https://upload.wikimedia.org/wikipedia/commons/d/db/Patern_test.jpg
Resolving upload.wikimedia.org (upload.wikimedia.org)... 91.198.174.208, 2620:0:862:ed1a::2:b
Connecting to upload.wikimedia.org (upload.wikimedia.org)|91.198.174.208|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 36623 (36K) [image/jpeg]
Saving to: ‘Patern_test.jpg’

Patern_test.jpg                  100%[===================================================================>]  35.76K  --.-KB/s    in 0.09s

2022-01-17 23:28:33 (417 KB/s) - ‘Patern_test.jpg’ saved [36623/36623]

┌──(root㉿ 0men)-[~/steghide]
└─# ls
message.txt  Patern_test.jpg
┌──(root㉿ 0men)-[~/steghide]
└─# ▬
```

- **Hide secret message in image and create a new encrypted file.**

This command will embed the file message.txt in the Patern_test.jpg and create a new encrypted image, secret.jpg (stego file).

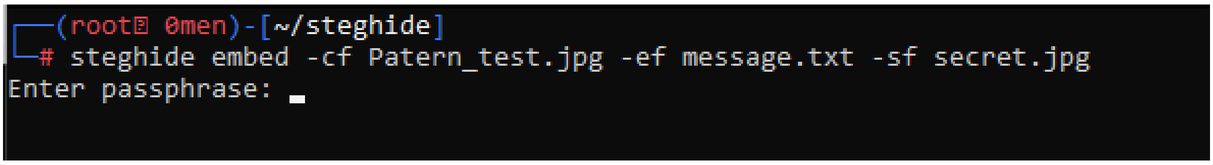
```
steghide embed -cf Patern_test.jpg -ef message.txt -sf secret.jpg
```

- Embed: embed data
- -cf: cover file
- -ef: embed file
- -sf: output file – stego file

You can also choose between different encryption algorithms and compression levels. See the user manual of steghide with:

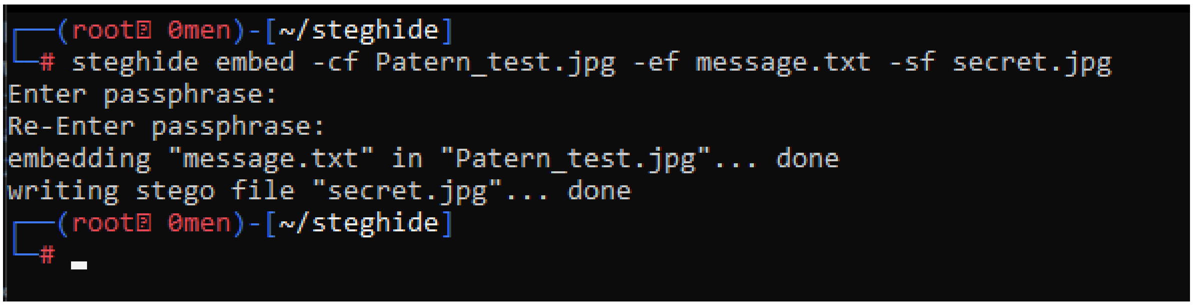
```
man steghide
```

- **It will prompt you to enter a passphrase needed to then later extract the message.txt from the secret.jpg image.**



```
┌──(root㉿ 0men)-[~/steghide]
└─# steghide embed -cf Patern_test.jpg -ef message.txt -sf secret.jpg
Enter passphrase: ▬
```

- **Enter a passphrase and re-enter it for confirmation** – be sure to remember it because you will not be able to decode the secret message from the stego file.



```
┌──(root㉿ 0men)-[~/steghide]
└─# steghide embed -cf Patern_test.jpg -ef message.txt -sf secret.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "message.txt" in "Patern_test.jpg"... done
writing stego file "secret.jpg"... done
┌──(root㉿ 0men)-[~/steghide]
└─# ▬
```

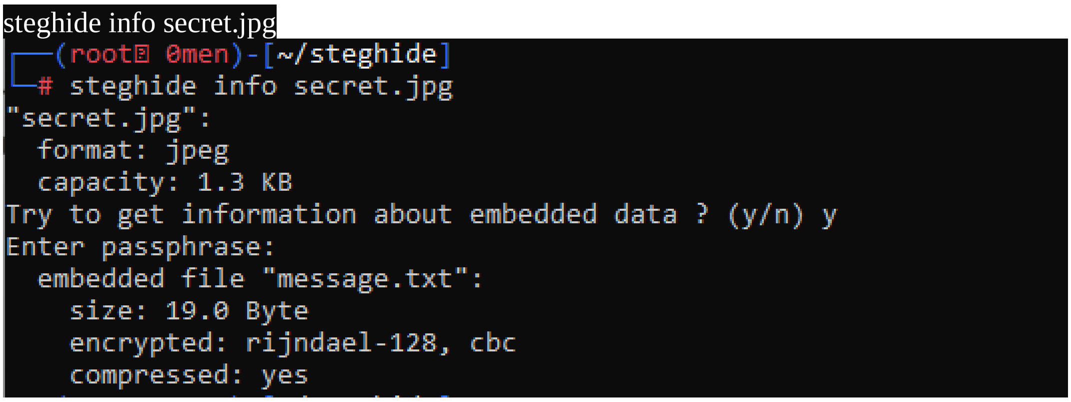
Now, the stego file (secret.jpg) is ready.

- **View info or the embedded data**

  You can get some information before extracting the stego file. To view the **encryption algorithm, file size, and the embedded filename/secret message filename** using the command below:

  (You must then enter the passphrase to continue)

```
steghide info secret.jpg
```

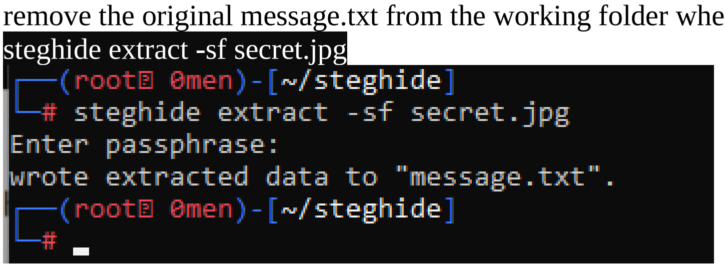


```
┌──(root□ 0men)-[~/steghide]
└─# steghide info secret.jpg
"secret.jpg":
  format: jpeg
  capacity: 1.3 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "message.txt":
    size: 19.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

- **Retrieve information of the embedded file (stego file)**

The way to decode and reveal the secret message embed in the stego file. Make sure to rename or remove the original message.txt from the working folder when performing this command.

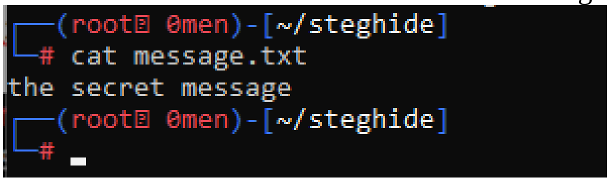
```
steghide extract -sf secret.jpg
```



```
┌──(root□ 0men)-[~/steghide]
└─# steghide extract -sf secret.jpg
Enter passphrase:
wrote extracted data to "message.txt".
┌──(root□ 0men)-[~/steghide]
└─# ▬
```

- Now the extracted message can be read and found in the working folder.

Use cat to read and confirm the embedded message.

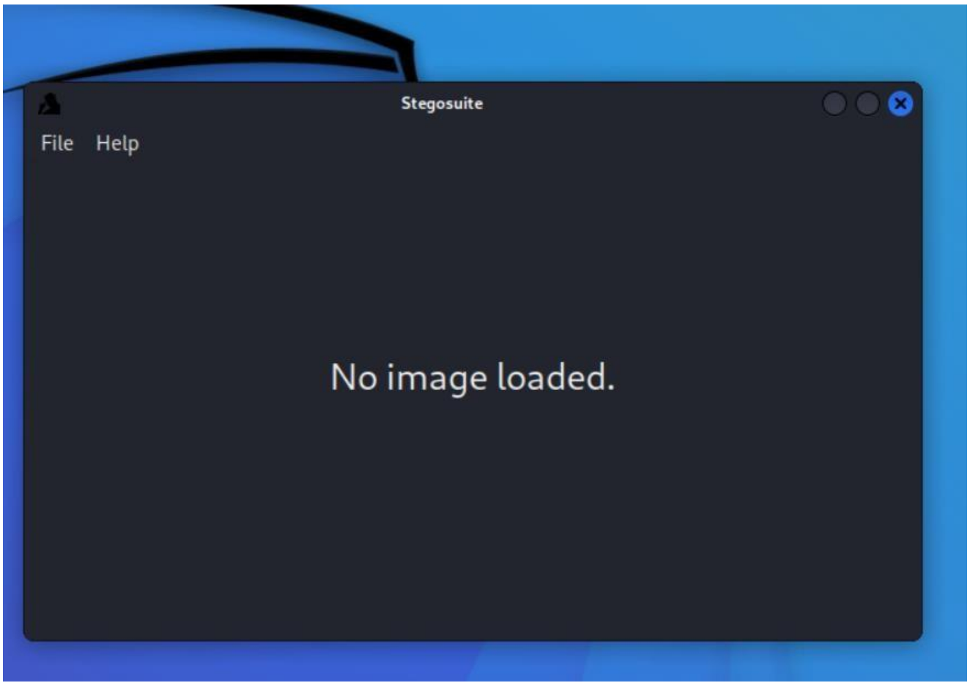


```
┌──(root□ 0men)-[~/steghide]
└─# cat message.txt
the secret message
┌──(root□ 0men)-[~/steghide]
└─# ▬
```

2.**Stegosuite**: Is a graphical interface steganographic tool written in Python for hiding data/extracting data them from images and more features.

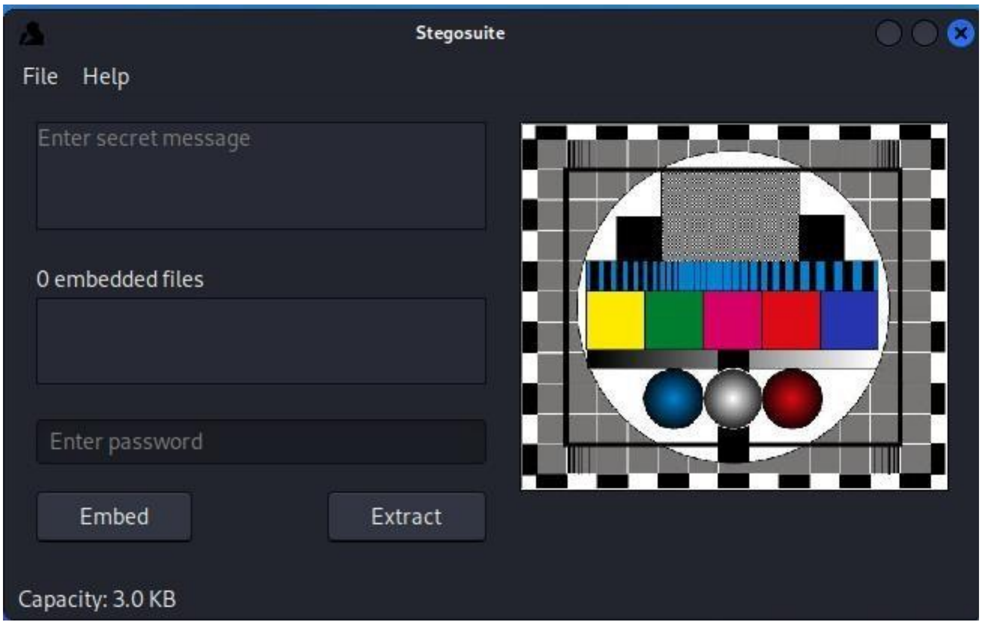
**Creating an image with a secret message in it.**
**It's a way easier method since no prior knowledge of bash scripting or terminal is required.**

- Run the tool from the terminal by typing stegosuite in the terminal and then click enter or you can find it from the navigation menu.



No image loaded.

- Click file from the menu bar and choose the image to hide the secret message



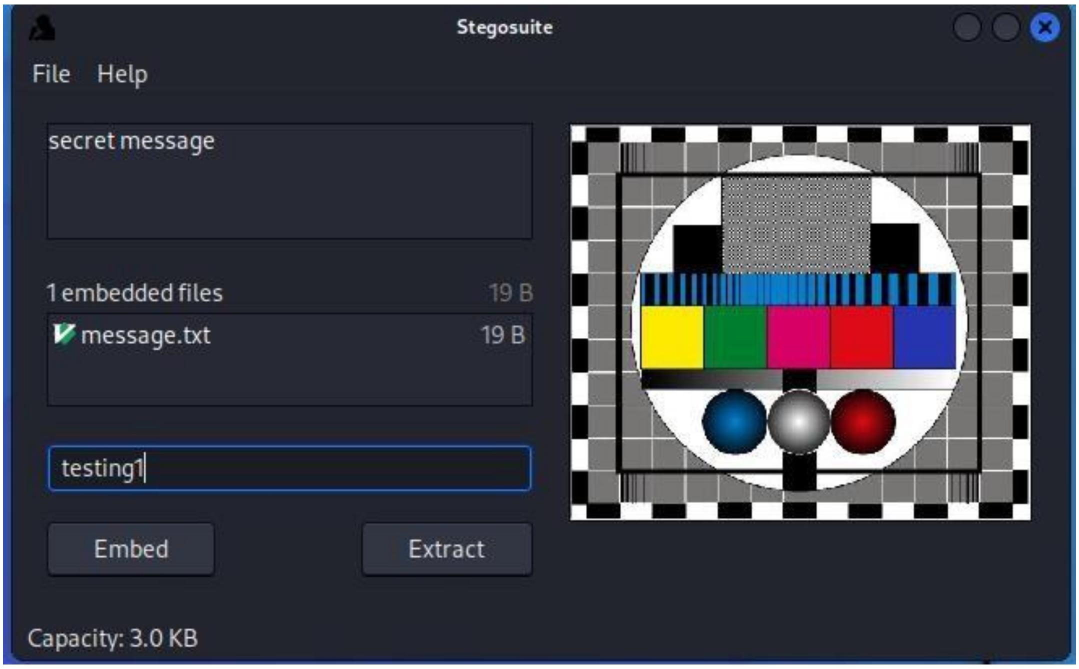
Enter secret message

0 embedded files

Enter password

Capacity: 3.0 KB

- You then just type the secret message, add the secret message.txt file (right click on the embedded files and add it) that you want to embed, enter a password and click Embed.



secret message

1 embedded files 19 B

message.txt 19 B

testing1

Capacity: 3.0 KB

- **The stego file will be created on the same directory where the image was saved with the name _embed on the end.**

  e.g. original filename: test.jpg will be test_embed.jpg

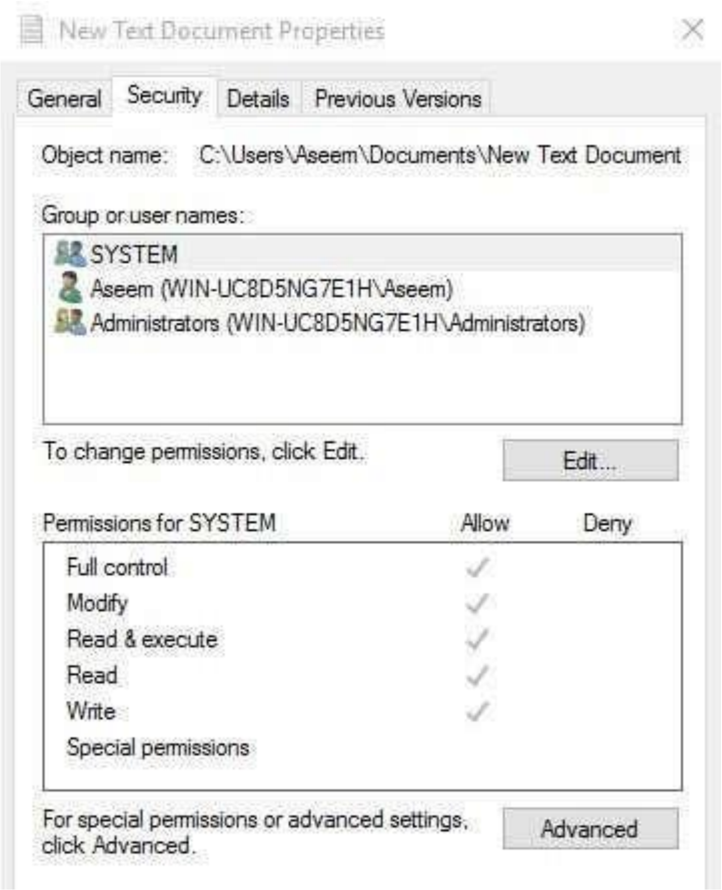
- **To extract the message just add the stego file from the file option on the header menu, type the password and click Extract.**

- **The secret message file will be saved also in the same directory where the stego file was saved with the same name that was embedded.**

Q6.Apply security to Files/ Folder/ Application using access permissions

Ans.6

Now that we got all of that out of the way, let’s talk about permissions in Windows. Every file and every folder in Windows has its own set of permissions. Permissions can be broken down into **Access Control Lists** with users and their corresponding rights. Here is an example with the user list at the top and the rights at the bottom:



Object name: C:\Users\Aseem\Documents\New Text Document

Group or user names:

- SYSTEM
- Aseem (WIN-UC8D5NG7E1H\Aseem)
- Administrators (WIN-UC8D5NG7E1H\Administrators)

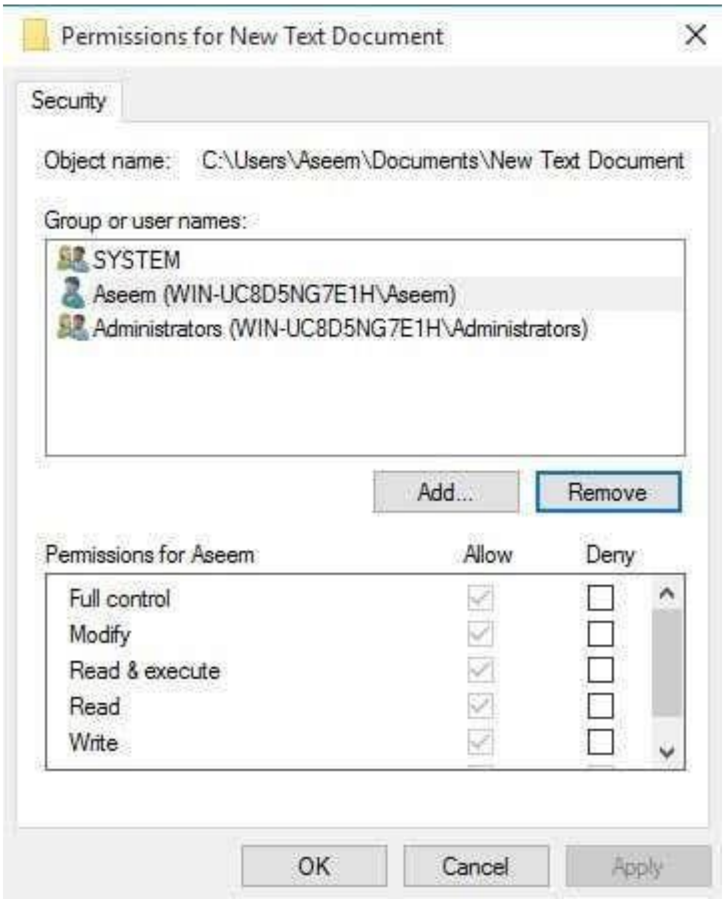
To change permissions, click Edit.

| Permissions for SYSTEM | Allow | Deny |
|---|---|---|
| Full control | ✓ | |
| Modify | ✓ | |
| Read & execute | ✓ | |
| Read | ✓ | |
| Write | ✓ | |
| Special permissions | | |

For special permissions or advanced settings, click Advanced.

Permissions are also either inherited or not. Normally in Windows, every file or folder gets their permissions from the parent folder. This hierarchy keeps going all the way up to the root of the hard drive. The simplest permissions have at least three users: SYSTEM, currently logged in user account and the Administrators group.

These permissions usually come from the **C:\Users\Username** folder on your hard drive. You can access these permissions by right-clicking on a file or folder, choosing **Properties** and then clicking on the **Security** tab. To edit permissions for a particular user, click on that user and then click the **Edit** button.



Object name: C:\Users\Aseem\Documents\New Text Document

Group or user names:

- SYSTEM
- Aseem (WIN-UC8D5NG7E1H\Aseem)
- Administrators (WIN-UC8D5NG7E1H\Administrators)

| Permissions for Aseem | Allow | Deny |
|---|---|---|
| Full control | ☑ | □ |
| Modify | ☑ | □ |
| Read & execute | ☑ | □ |
| Read | ☑ | □ |
| Write | ☑ | □ |

Note that if the permissions are greyed out, like in the example above, the permissions are being inherited from the containing folder. I'll talk about how you can remove inherited permissions further below, but first let's understand the different types of permissions.

Q7.Study of System threat attacks - Denial of Services.

## Ans 7. Denial-of-service attack?

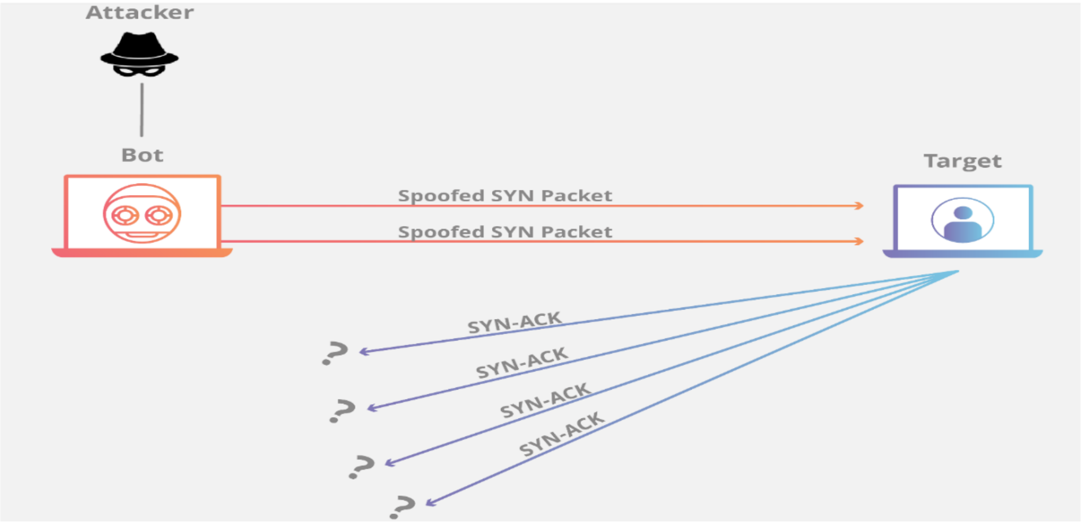
A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

## Common denial-of-service attacks?

There are many different methods for carrying out a DoS attack. The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic. These service requests are illegitimate and have fabricated return addresses, which mislead the server when it tries to authenticate the requestor. As the junk requests are processed constantly, the server is overwhelmed, which causes a DoS condition to legitimate requestors.

- In a **Smurf Attack**, the attacker sends Internet Control Message Protocol broadcast packets to a number of hosts with a spoofed source Internet Protocol (IP) address that belongs to the target machine. The recipients of these spoofed packets will then respond, and the targeted host will be flooded with those responses.
- A **SYN flood** occurs when an attacker sends a request to connect to the target server but does not complete the connection through what is known as a three-way handshake—a method used in a Transmission Control Protocol (TCP)/IP network to create a connection between a local host/client and server. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect.

Individual networks may be affected by DoS attacks without being directly targeted. If the network's internet service provider (ISP) or cloud service provider has been targeted and attacked, the network will also experience a loss of service.



Q8. Study of Techniques uses for Web Based Password Capturing.
Ans 8. Techniques uses for web based password capturing are:

## 1. Phishing

There’s an easy way to hack, ask the user for his or her password. A phishing email leads the unsuspecting reader to a spoofed log in page associated with whatever service it is the hacker wants to access, usually by requesting the user to put right some terrible problem with their security. That page then skims their password and the hacker can go use it for their own purpose.

## 2. Social Engineering

Social engineering takes the whole “ask the user” concept outside of the inbox that phishing tends to stick with and into the real world.

A favorite of the social engineer is to call an office posing as an IT security tech guy and simply ask for the network access password. You’d be amazed at how often this works. Some even have the necessary gonads to don a suit and name badge before walking into a business to ask the receptionist the same question face to face.

Time and again, it’s been shown that many businesses either don’t have good security in place or people are too friendly and trusting when they shouldn’t be, such as giving people access to sensitive locations because of a uniform or sob story.

## 3. Malware

Malware comes in many forms, such as a keylogger, also known as a screen scraper, which records everything you type or takes screenshots during a login process, and then forwards a copy of this file to hacker central.

Some malware will look for the existence of a web browser client password file and copy it, which, unless properly encrypted, will contain easily accessible saved passwords from the user’s browsing history.

## 4. Dictionary Attack

The dictionary attack uses a simple file containing words that can be found in a dictionary, hence its rather straightforward name. In other words, this attack uses exactly the kind of words that many people use as their password.

Cleverly grouping words together such as “letmein” or “superadministratorguy” will not prevent your password from being cracked this way – well, not for more than a few extra seconds.

## 5. Rainbow Table Attack

Rainbow tables aren’t as colorful as their name may imply but, for a hacker, your password could well be at the end of it. In the most straightforward way possible, you can boil a rainbow table down into a list of pre-computed hashes – the numerical value used when encrypting a password. This table contains hashes of all possible password combinations for any given hashing algorithm. Rainbow tables are attractive as it reduces the time needed to crack a password hash to simply just looking something up in a list.

However, rainbow tables are huge, unwieldy things. They require serious computing power to run and a table becomes useless if the hash it's trying to find has been "salted" by the addition of random characters to its password ahead of hashing the algorithm.

There is talk of salted rainbow tables existing, but these would be so large as to be difficult to use in practice. They would likely only work with a predefined "random character" set and password strings below 12 characters as the size of the table would be prohibitive to even state-level hackers otherwise.

## 6. Spidering

Savvy hackers have realized that many corporate passwords are made up of words that are connected to the business itself. Studying corporate literature, website sales material, and even the websites of competitors and listed customers can provide the ammunition to build a custom word list to use in a brute force attack.

Really savvy hackers have automated the process and let a spidering application, similar to the web crawlers employed by leading search engines to identify keywords, and then collect and collate the lists for them.

## 7. Offline Cracking

It's easy to imagine that passwords are safe when the systems they protect lock out users after three or four wrong guesses, blocking automated guessing applications. Well, that would be true if it were not for the fact that most password hacking takes place offline, using a set of hashes in a password file that has been 'obtained' from a compromised system.

Often the target in question has been compromised via a hack on a third party, which then provides access to the system servers and those all-important user password hash files. The password cracker can then take as long as they need to try and crack the code without alerting the target system or individual user.

## 8. Brute Force Attack

Similar to the dictionary attack, the brute force attack comes with an added bonus for the hacker. Instead of simply using words, a brute force attack lets them detect non-dictionary words by working through all possible alpha-numeric combinations from aaa1 to zzz10.

It's not quick, provided your password is over a handful of characters long, but it will uncover your password eventually. Brute force attacks can be shortened by throwing additional computing horsepower, in terms of both processing power – including harnessing the power of your video card GPU – and machine numbers, such as using distributed computing models like online bitcoin miners.

## 9. Shoulder Surfing

Another form of social engineering, shoulder surfing, just as it implies, entails peeking over a person's shoulders while they're entering credentials, passwords, etc. Although the concept is very low tech, you'd be surprised how many passwords and sensitive information is stolen this way, so remain aware of your surroundings when accessing bank accounts, etc. on the go.

The most confident of hackers will take the guise of a parcel courier, aircon service technician, or anything else that gets them access to an office building. Once they are in, the service personnel "uniform" provides a kind of free pass to wander around unhindered, and make note of passwords being entered by genuine members of staff. It also provides an excellent opportunity to eyeball all those post-it notes stuck to the front of LCD screens with logins scribbled upon them.

## 10. Guess

The password crackers’ best friend, of course, is the predictability of the user. Unless a truly random password has been created using software dedicated to the task, a user-generated ‘random’ password is unlikely to be anything of the sort.

Instead, thanks to our brains’ emotional attachment to things we like, the chances are those random passwords are based upon our interests, hobbies, pets, family, and so on. In fact, passwords tend to be based on all the things we like to chat about on social networks and even include in our profiles. Password crackers are very likely to look at this information and make a few – often correct – educated guesses when attempting to crack a consumer-level password without resorting to dictionary or brute force attacks.

Q9. Study of Anti-Intrusion Technique – Honey pot.
Ans 9.

## Honeypot

A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your security policies. You can apply a honeypot to any computing resource from software and networks to file servers and routers.

Honeypots are a type of deception technology that allows you to understand attacker behavior patterns. Security teams can use honeypots to investigate cybersecurity breaches to collect intel on how cybercriminals operate. They also reduce the risk of false positives, when compared to traditional cybersecurity measures, because they are unlikely to attract legitimate activity.

Honeypots vary based on design and deployment models, but they are all decoys intended to look like legitimate, vulnerable systems to attract cybercriminals.

## Working of Honeypot

A honeypot trap can be manufactured to look like a payment gateway, which is a popular target for hackers because it contains rich amounts of personal information and transaction details, such as encoded credit card numbers or bank account information. A honeypot or honeynet can also resemble a database, which would lure actors that are interested in gathering intellectual property (IP), trade secrets or other valuable sensitive information. A honeypot may even appear to contain potentially compromising information or photos as a way to entrap adversaries whose goal is to harm the reputation of an individual or engage in ransomware techniques.

Once inside the network, it is possible to track cybercriminals' movements to better understand their methods and motivations. This will help the organization adapt existing security protocols in order to thwart similar attacks on legitimate targets in the future.

To make honeypots more attractive, they often contain deliberate but not necessarily obvious security vulnerabilities. Given the advanced nature of many digital adversaries, it is important for organizations to be strategic about how easily a honeypot can be accessed. An insufficiently secured network is unlikely to trick a sophisticated adversary and may even result in the bad actor providing misinformation or otherwise manipulating the environment to reduce the efficacy of the tool.

## Types of Honeypot

- **Email traps** or spam traps place a fake email address in a hidden location where only an automated address harvester will be able to find it. Since the address isn't used for any purpose other than the spam trap, it's 100% certain that any mail coming to it is spam. All messages which contain the same content as those sent to the spam trap can be automatically blocked, and the source IP of the senders can be added to a denylist.
- A **decoy database** can be set up to monitor software vulnerabilities and spot attacks exploiting insecure system architecture or using SQL injection, SQL services exploitation, or privilege abuse.

- A **malware honeypot** mimics software apps and APIs to invite malware attacks. The characteristics of the malware can then be analyzed to develop anti-malware software or to close vulnerabilities in the API.

- A **spider honeypot** is intended to trap WebCrawler’s ('spiders') by creating web pages and links only accessible to crawlers. Detecting crawlers can help you learn how to block malicious bots, as well as ad-network crawlers.

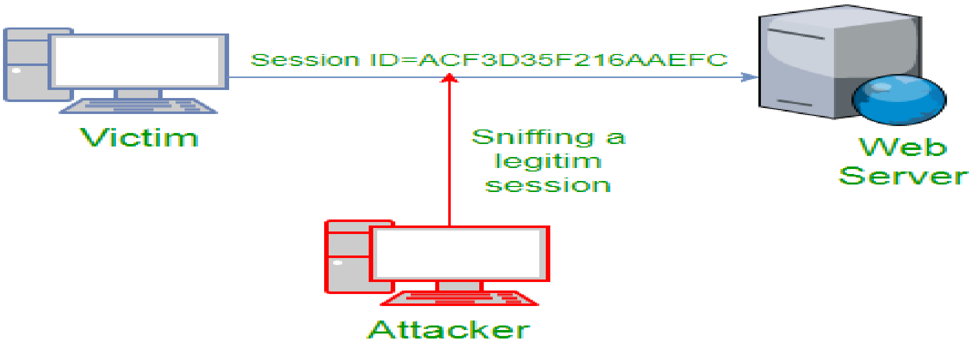
Q10. Study of Sniffing and Spoofing attacks.
Ans 10.

## IP Sniffing and IP Spoofing

In sniffing, an attacker falsifies the authorized readers, that can scan the legal tags to acquire valuable data. In spoofing attacks, an attacker efficaciously fakes as an official and legal operator of a system. The duplicating factor of a spoofing attack is an approved user of a system. Spoofing attacks are not the same as the other attacks such as counterfeiting or sniffing. However, counterfeiting, packet-sniffing, and spoofing all fall under the ambit of misrepresentation and deception kinds of attack.

## Sniffing

The practice or technique of monitoring, gathering, capturing, and logging some or all data packets passing through a given computer network is called sniffing or packet sniffing. A packet sniffer is composed of two parts namely; a network adapter and software that is used by a network to observe or troubleshoot network traffic.

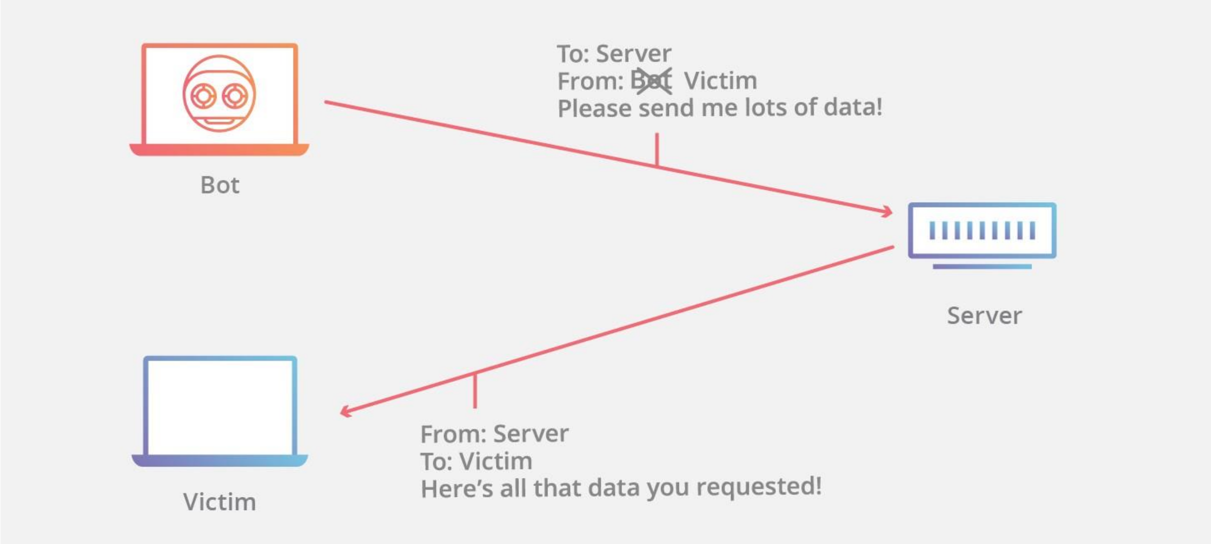


Attackers use these sniffers to seize data packets that contain valuable information and analyze the network traffic. Sniffing is categorized into active sniffing and passive sniffing. In Active sniffing, there is the constant activity by the attacker to obtain information and sniff the traffic from the switch network. In passive sniffing, the attacker is hidden and sniffs through the hub.

## Spoofing

Any kind of behavior where an attacker mask as an authentic user or a device to secure something beneficial or crucial information for their gain is called spoofing. There are various kinds of spoofing such as website spoofing, E-mail spoofing, and IP spoofing. Other common methods include ARP spoofing attacks and DNS server spoofing attacks.

An E-mail spoofing targets the user while an IP spoofing is predominantly targeted at a network.
In an IP spoofing attack, the attacker attempts to obtain illicit and illegal access to a network through messages with a bogus or spoofed IP address to deceive and show it off as a message from a trusted source. This is achieved by using a genuine host's IP address and varying the packet headers led from their personal system to mimic it as an original and a trusted computer's IP address.


Bot
To: Server
From: ~~Bot~~ Victim
Please send me lots of data!
Server
Victim
From: Server
To: Victim
Here's all that data you requested!