System Hacking

Module 5

System Hacking

Learning Objective

1. Define system hacking
2. Explain the various types of system hacking
3. Identify steganography
4. Explain the various types of steganography
5. Describe steganalysis
6. Understand password cracking and the various tools involved in it
7. State the various types of password attacks
8. State the importance of covering tracks after a hack
9. Describe different ways to cover online tracks

System Hacking 1-2

- In System hacking:
  - Scanning and enumeration are the initial stages of hacking, this is where the groundwork for hacking is started.
  - The procedure through which an individual tries to break into a system to gain access is known as system hacking.
  - During enumeration, the hacker acquires all the information necessary for system hacking.
  - The owners or users of systems provide their consent to hackers to perform this activity on their systems in ethical system hacking.

System Hacking 2-2

- System hacking:
  - Is aimed at collecting sufficient information by gaining access over the user system, by using techniques such as brute force.
- After gaining access to the users' system the hacker can also carry out malicious activities, such as:
  - Escalating privileges of the users by cracking their passwords.
  - Executing applications by creating and maintaining backdoor access.

System Hacking Methodology 1-2

- Hacking is today rampant all over the world and poses a threat to many individuals as well as companies.
- To counter these threats, it is important to know how hacking works.

System Hacking Methodology 2-2

- Hackers:

Step 1	• Zero-in on a computer or network they wish to target.
Step 2	• Map the targeted computer or network. (This step includes mapping the vulnerabilities of the system and gaining access to it.)
Step 3	• Gain access by cracking passwords, by spoofing the IP address of the targeted network or personal computer of the individual or company, or by conducting stack-smashing attacks.
Step 4	• 'Sniff' the internal network for vital data of the user or the company after mapping the target.
Step 5	• Can cover their tracks to ensure the hacked data does not lead back to them after hacking is done.

Steganography

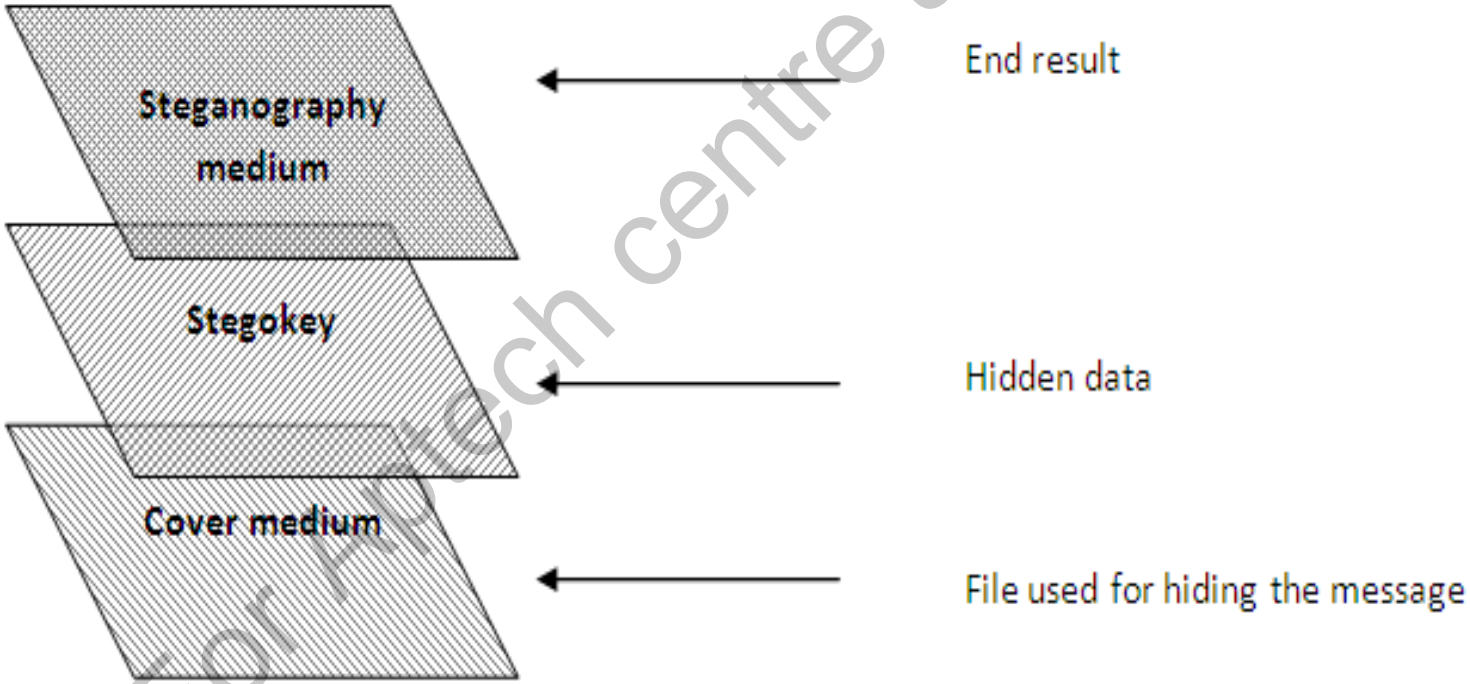
- **Steganography:**
  - Derived from the Greek word '*steganos*' meaning covered and '*graphy*' meaning writing.
  - Involves layering the target data, such as an image or audio file and inserting data into it.
  - Reveal data using specific steganography software.
  - Has a stegokey as a password or a secret message concealed with the help of an image file, an audio file, or any other type of media file that can act as a medium for transmitting the file.

Steganography Techniques 1-2

- **Steganography:**
  - Is the art of concealing ongoing communication being conducted through media files, folders, e-mails and so on.
  - Helps various applications to employ varied aspects of the steganography technique.
  - Has instances where some applications may require total invisibility of the secret information, whereas others may require only a large chunk of the secret message to be hidden.

Steganography Techniques 2-2

- The following figure displays the steganography process:

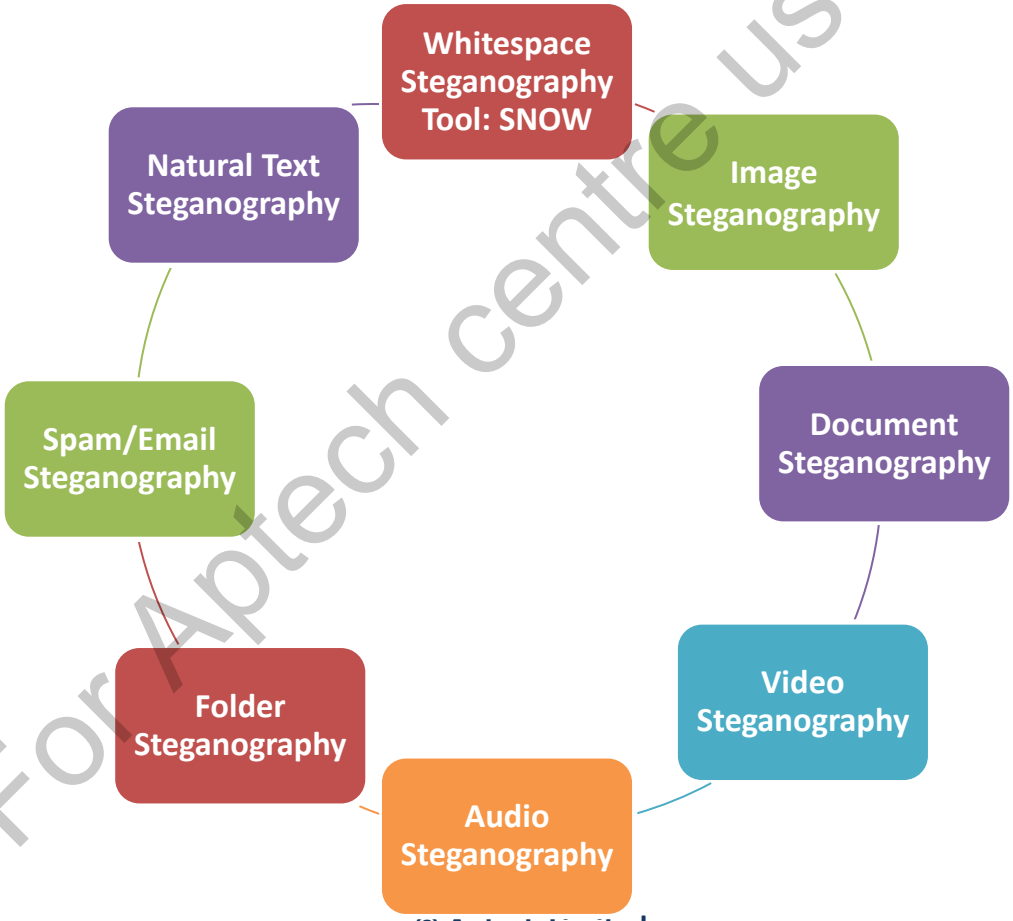


Types of Steganography 1-2

Steganography is the process of hiding certain data in other types of data such as test files or images in order to communicate and covert message to the receiver.

Types of Steganography 2-2

- Following are some of the common types of steganography:



Whitespace Steganography Tool: SNOW 1-2

- **SNOW:**

Is a program used for extracting and concealing messages in ASCII (American Standard Code for Information Interchange) text files.	Hides messages by appending or attaching spaces and tabs, better known as whitespace, at the end of lines.

- Most viewers cannot differentiate these spaces and tabs, thus making these files difficult to decipher.

Whitespace Steganography Tool: SNOW 2-2

- The options available in SNOW include:

-C	• Stands for compress. This option compresses the file during hiding and uncompresses the file while extracting it.
-Q	• Stands for quiet mode. This mode is used to turn off verbose messages when the program is running.
-S	• Stands for show. This option shows the approximate space available in the cover file.
-p	• Stands for password. This option is used for decryption.
- l	• Stands for line length. Using this option, SNOW creates lines shorter than this parameter.
-f	• Stands for a message-file. This is the actual file that is concealed.
-m	• Stands for a message string. This is the secret message string.

Image Steganography 1-3

- Images are commonly used for hiding data.
- An attacker merely has to embed the information into the image using any one of the following methods:

LSB Substitution:

- LSB stands for least-significant-bit.
- As the name signifies, the least-significant-bits of the image are replaced with message bits.
- However, this form of image steganography is vulnerable to even the slightest image manipulation.
- For instance, when an image is converted from GIF format to JPEG format, the probability of its getting lost is very high.

Image Steganography 2-3

Blocking:

- Blocking means disintegrating an image into ‘blocks’.
- These blocks are disintegrated or broken down using Discrete Cosine Transforms (DCT).
- Each block is broken into 64 DCT coefficients that imitate the colour and luminance of the image.
- These DCT coefficients are then modified to conceal the secret message.

Palette Modification:

- A particular palette of colours is used to make up an image.
- This palette serves as a characteristic of the image, which cannot be replicated.
- Steganography software, such as HideSeek, makes entries into the colour palette.
- These entries are divisible by four.
- This palette modification creates a palette signature that represents the hidden messages.

Image Steganography 3-3

Hiding Messages in Images:

- A software called QuickStego helps in hiding messages in images.
- The following figure gives a screenshot of an image steganography using QuickStego:

Document Steganography

- **In Document Steganography:**
  - 'Tabs' and 'white spaces' are added to the data.
  - This is one of the easiest ways of carrying out steganography as whites spaces and tabs are not visible in text view.
  - Another form of document-based or text-based steganography is using selective characters for transmitting a message through some other text or document.
  - For example: Consider the following sentence:

    'Meet at noon during Opera with net'

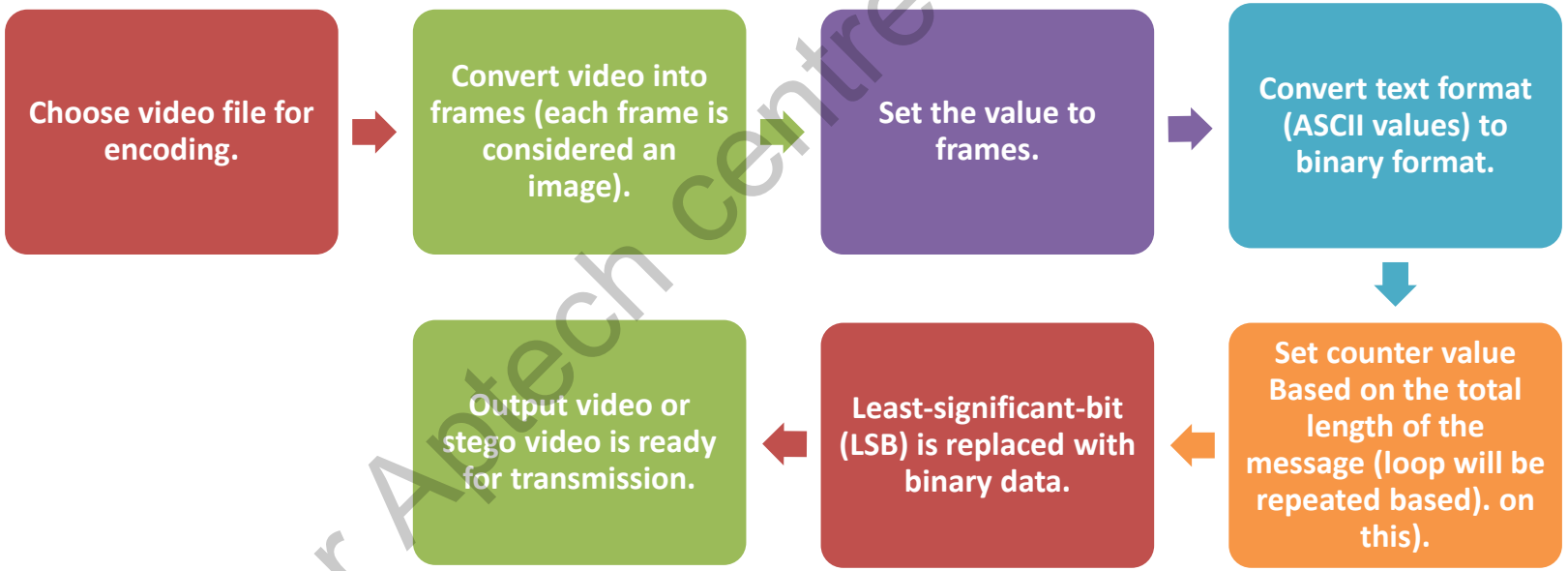
  - Here, if you place the first letters of each word together, you get the message 'Man Down'.
  - Such messages can be transmitted easily without being divulged.

Video Steganography 1-3

- Video steganography involves the addition of a stegokey to the video file.
- The LSB technique used in image steganography can also be used in video steganography.
- While in image steganography, the palette or pixels are tampered with, in video steganography, the frames of the video are tweaked.
- Firstly, the video file is encoded to ensure that the video output is proper and does not seem tampered.

Video Steganography 2-3

- In the following figure shows the steps for encoding a video file.



Video Steganography 3-3

- The decoding of a video is to some extent the reverse of the encoding process.
- For decoding, the counter of the binary LSB encoded is set.
- This data is then extracted from the LSB encoded image by removing the LSBs of the pixels in the image.
- To form the text from the binary data, all the binary bits need to be grouped.

Audio Steganography 1-6

- **In Audio Steganography:**
  - The signals are modified in order to transmit hidden information.
  - Steganography aims at ensuring that the secret data is covered with the help of a medium, such that the resultant output does not have any noticeable changes.
  - This method relies on the psycho-acoustical masking phenomenon of the Human Auditory System (HAS), which has a very low differential range.
  - In other words, in the presence of a strong tone, it is difficult to identify a weaker one, as the stronger tone masks the weaker tone.

Audio Steganography 2-6

- Audio masking usually takes place when the human ear finds it difficult to perceive weaker tones in the presence of a stronger tone, more so within a critical band.

- This aspect is beneficial for audio steganography.

Audio Steganography 3-6

- Some of the techniques used in audio steganography are as follows:

Least Significant Bit (LSB)

- LSB coding is the simplest way of embedding information in an audio file.
- Similar to video and image steganography, in audio steganography the LSB of a sampling point is replaced with a binary message.
- In case of certain LSB codes, the LSBs are substituted with message bits.
- This diversifies the data to be encoded and increases the amount of noise in the audio file.
- To decode the audio message, the receiver of the file must have access to the sequence of sample indices that have been used in the embedding process.
- The length of the secret message is usually smaller than the total number of samples present in a sound file.

Audio Steganography 4-6

Spread Spectrum

- Spread Spectrum works on the principle that increasing the signal bandwidth in channels with narrowband noise increases the transmitted signal bandwidth.
- This further increases the possibility that the information received will be correct.
- Some of the common Spread Spectrum techniques are Time Hopping Spread Spectrum (THSS), Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).
- Each of these techniques have different implementation techniques.

Audio Steganography 5-6

Echo Hiding

- In echo hiding, as the name suggests, the secret data is concealed in the echo of the source audio.
- An artificial echo is fabricated to conceal the initial amplitude, the delay and the data.
- The delay between the fabricated echo and the original audio makes it difficult to differentiate between the two signals.
- Moreover, the echo is mistaken to be just an extra resonance.
- In echo hiding, the original signal is broken into smaller blocks. After the encoding process, these blocks are linked together to form the final signal.

Audio Steganography 6-6

- Audio steganography is more difficult than image steganography, as the auditory senses of human beings are relatively stronger than their visual senses.
- Thus, while embedding a file into an audio file, one must ensure that the header of the audio file is intact.
- If the first 44 bytes of the audio file are tampered with, there is a high probability of the audio file becoming corrupt.
- In addition, the secret file must not be embedded in the silent zone of the audio file as this could change the audio file itself.

Folder Steganography 1-2

- **In Folder Steganography:**
  - Files are concealed inside a folder.
  - Although, it is possible to conceal files in folders using the hidden attribute, in folder steganography, the file is physically moved but is still linked to the folder.
  - The hidden files are not visible in windows-based applications, such as Windows Explorer, and they cannot be accessed without a password.
  - Moreover, the viewer may not even know that the folder contains any hidden files.

Folder Steganography 2-2

- In the figure displays a screenshot of InvisibleSecrets, the software that helps in conducting steganography for files, audio files and e-mails:

Spam/E-mail Steganography

- **E-mail or Spam Steganography:**
  - Can be conducted by using the timing of an e-mail rather than its contents.
  - Difficult to detect an e-mail with embedded information.
  - Is done by analysing the e-mails on the network for any steganographic messages that may be embedded in them.

- One such technique is the Simple Mail Transfer Protocol (SMTP) transaction capture that detects any steganographic information within a network.
- After detection, the message is stored in a database and then extracted to reveal the original message.

Natural Text Steganography

- Natural text steganography is the process of concealing data in a text-based document.
- Some text-based steganography techniques use random word and character sequences, shifting words, feature coding and so on.
- In case of character sequencing, characters are randomly positioned to ensure that it becomes difficult for the attacker to break through the concealed message.

Steganalysis: Concept 1-2

- **Steganalysis:**
  - Is the study of identifying concealed messages using steganography.
  - Is often confused with cryptanalysis, the two are different.
  - Help user to ascertain whether the data contains any hidden message.
  - Helps a steganalyst or an individual who analyses files for concealed information, firstly reduces the data files into a subset, which is more likely to contain the hidden message.

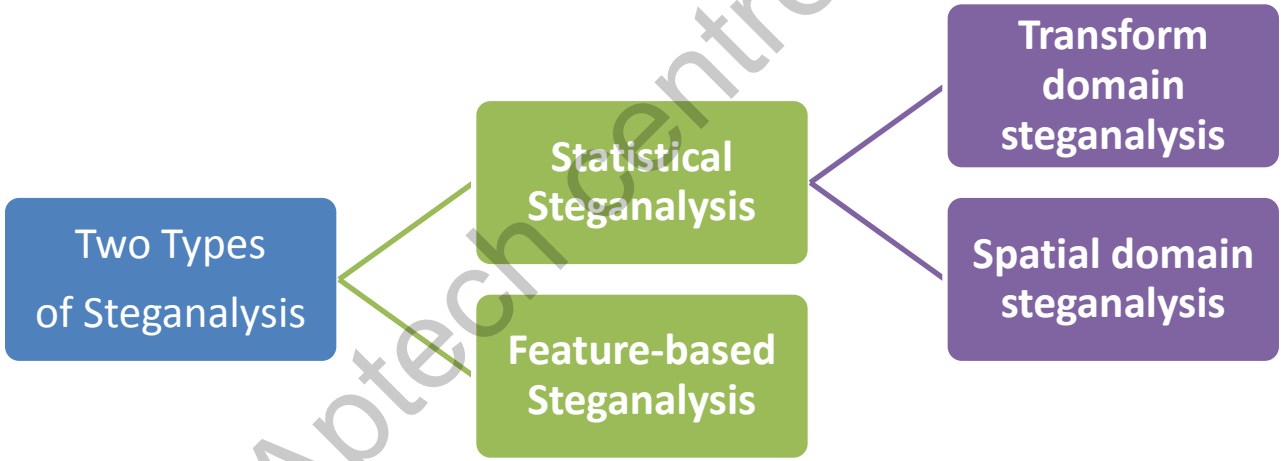
Steganalysis: Concept 2-2

- The widespread knowledge of steganography and steganalysis has resulted in many companies and individuals wanting to secure their vital information.

- There is also a surge in the number of people interested in spotting the data as most of this information may relate to illegal activities.

Steganalysis Methods 1-3

- On the basis of the process used to detect the concealed message, steganalysis can be divided into two methods:



Steganalysis Methods 2-3

- **Statistical Steganalysis**:
  - Is carried out with the help of pixels.
  - Is classified into the following:

Transform Domain Steganalysis

- In this type of statistical analysis, the frequency counts of coefficients are computed.
- Thereafter, a histogram analysis is carried out to differentiate between the stego image and the cover image.
- A drawback of this method is its inability to provide details about the embedding algorithms.

Spatial Domain Steganalysis

- In this type of statistical analysis, the first step is to analyse a pair of pixels and spot the difference between them.
- Once the pixels are analysed, a histogram is plotted to reveal the concealed message.

Steganalysis Methods 3-3

- **Feature-based Steganalysis**:
  - The features of the data are extracted for choosing and preserving the information in addition to detecting the concealed message.
  - Can be used for training classifiers.

Steganalysis Attacks 1-2

- A steganalysis attack is based on the information available to the attacker or the steganalyst.

- Some common types of steganalysis attacks and their descriptions are as follows:

Type of Steganalysis Attack	Description
Steganography-only attack	This consists of detecting the concealed information based on data transfer without making assumptions about the steganography algorithm that is applied. In this type of attack, only the medium of steganography is available for analysis.
Known-carrier attack	In this attack, both the medium of steganography and the cover are available for analysis.

Steganalysis Attacks 2-2

Type of Steganalysis Attack	Description
Known-message attack	In this attack, the attacker is aware of the hidden message, but is not chosen by him.
Chosen-steganography attack	The attacker is aware of the medium and the algorithm.
Chosen-message attack	Known-messages and algorithms are used to create a steganographic medium for comparing and analysing. This technique is used to determine the equivalent pattern that provides directives for steganography algorithms.
Known-steganography attack	The attacker is aware of the carrier, the medium and the algorithm.

Steganography Detection Tools 1-2

- Some common steganography detection tools include:
  - Stegdetect
  - Xstegsecret
  - StegSpy
  - Stego Watch
  - StegAlyzerAS
  - StegAlyzerRTS
  - StegMark
- Stegdetect:
  - Initially determines the linear detection function that can be implementing for images that have not been classified yet.
  - Calculates the hyperplane that separates stego images from non-stego images.

Steganography Detection Tools 2-2

– The following figure shows an example of Stegdetect software:

```
$ stegdetect *.jpg
Girl.jpg : outguess(old)(***) jphide(*)
Dscf1111.jpg : negative
Dscf2222.jpg : jsteg(***)
Dscf3333.jpg : jphide(***)
[...]
$ stegbreak -tj dscf2222.jpg
Loaded 1 files...
Dscf2222.jpg : jsteg(Dreamland)
Processed 1 files, found 1 embeddings.
Time: 37 seconds: Cracks: 358942,   9541 c/s
```

Password Cracking

- **Password Cracking:**
  - Is a process used in computer security.
  - Basically recovers passwords that have been stored in a computer or network.
  - Makes use of administrative privileges to recover lost passwords from a computer or a network.
  - Used by system administrators to track passwords that are easy to crack.
  - Used for legal purposes, especially in cases of restricted access to certain files that could be used as evidence in a court case.

Types of Password Attacks

- To understand password attacks, you must first be aware of the types of password attacks that are employed for garnering passwords.

- The two main types of password attacks are as follows:

Passive online attacks

Active online attacks

Passive Online Attacks 1-2

- **In Passive Attacks:**
  - The attacker does not contact the user to acquire the password.
  - The attacker covertly works on cracking the password without communicating with the user.

Passive Online Attacks 2-2

- Some common types of passive online attacks are:

Wire Sniffing

- In this attack, the hacker:
  - Uses a type of sniffing software to obtain user information.

Man-in-the-Middle (MITM)

- In this attack, hacker:
  - Acts as a middle-man who intercepts the authentication request.
  - Forwards the request to the server after interception.
  - Are in a position to tamper with both the connections as well as acquire the password.

Replay Attack

- In this attack, the hacker:
  - Intercepts the password authentication request and resends it to the server for further authentication.
  - Captures the password and reuses the password authentication request packers for later use.

Active Online Attack

- **In Active Online Attacks:**
  - Hackers attack computer systems that have poor or weak passwords.
  - Some common active online attacks include:

Trojan	• This type of malware appears harmless, but contains malicious codes that enter a computer through software add-ons.
Spyware	• This spying software works in the background, without the knowledge of the user, as it is not visible.
Keylogger	• This software process observes and saves keystroke events carried out by a user.
Hash Injection Attack	• In this type of attack, the attacker injects a compromised hash in the local session to use the same hash for validating the various network resources.

Rainbow Attacks: Pre-Computed Hash

- A rainbow table is a list of hashes that have been worked out in advance.
- These hashes are the numerical values of passwords.
- A rainbow table takes relatively less time to crack a password as compared to other types of password cracking tools.
- The only drawback in case of this technique is that it is time-consuming.
- Moreover, if the hashes that the rainbow table is trying to locate have random characters, also known as salting.
- Salting is carried out on passwords before the application of the hash algorithm.

Distributed Network Attack 1-2

- **Distributed Network Attacks (DNA):**
  - Are also known as Distributed Denial of Service (DDoS) attacks.
  - Banks on and attacks the Web resource.
  - Sends multiple requests to ensure that the Web site exceeds its capacity to handle the multitude of requests.
  - Is successful in preventing the Web site resource in functioning smoothly.

Distributed Network Attack 2-2

- Some common DNA attacks include:
  - Web sites of casinos
  - Online shopping companies
  - Companies that deal with online transactions

Non-Electronic Attacks 1-2

- In the Non-electronic attacks, the password hackers:
  - Hack passwords offline or in a non-electronic manner with the help of a set of hashes inserted in the password file.
  - Can leisurely crack the password without being threatened by any warnings of locking out the user on failed password attempts after obtaining this file from the user's system.

Non-Electronic Attacks 2-2

- Some common non-electronic attacks include:

Social Engineering	• The attacker poses as somebody else to acquire vital details of a user. • For example, the attacker may pose as a bank executive and ask for the customer's bank details.
Shoulder Surfing	• The attacker targets the location of the user. • In other words, the attacker visits the location in person and tries to garner maximum information and essential data that can help in planning the attack.

Manual Password Cracking (Guessing) 1-4

- **Manual Password Cracking (Guessing):**
  - Is one of the most primitive and easy ways of hacking into a system is guessing the password.
  - Is easier if the attacker knows the users and can easily guess the most probable password used by them, such as birth date, anniversary, mother or father's name, name of dog and so on.
  - Is the most common technique where hacker can keep a close eye on the information exchanged on social networking sites that may lead to the password used.
  - Helps the hacker to shortlist the most-probable passwords and guess the password used by a user.

Manual Password Cracking (Guessing) 2-4

- To expedite the password guessing process, hackers make use of automated tools.
- A common automated technique is using the Windows shell commands that are based on the standard NET USE syntax.

Manual Password Cracking (Guessing) 3-4

- To devise a script for guessing a password follow these steps:

1. Open Windows Notepad.
2. Create a username and password.
3. Automated tools such as dictionary generator can produce such word lists.
4. Save the file in *.txt format on the hard drive, preferably the C drive with the name details.txt
5. Use the FOR command to pipe the file C:\> FOR /F ‘token=1, 2*’ %i in (details.txt).
6. Type **net use \\targetIP\IPC$ %i /u: %j** to use the details.txt for using the *.txt file for logging on to the hidden share of the targeted system.

Manual Password Cracking (Guessing) 4-4

- **Biometrics or Smart Cards:**
  - Helps user to brace yourself against an automated password guessing attack.
  - Add a layer of security to the system as a user will need a fingerprint analysis via a biometric system to access a particular system.
  - Use a two-factor authentication for the purpose of identification.
  - Increases the security or lowers the susceptibility of any password attacks.

Stealing Passwords Using a USB Drive 1-3

- In an offline attack, A hacker steals passwords using a USB drive. To do so, hacker:
  - Copies password hacking software, such as messenPass or MailPassView, on a USB drive of capacity 1 GB or more. These software are small password recovery tools easily fit on a USB drive.
  - Creates a new notepad document and types the following text in it:

```
[autorun]

open=launch.bat

ACTION= Perform a virus scan
```

Stealing Passwords Using a USB Drive 2-3

- After saving the file as autorun.inf and copying it to the USB drive, the hacker opens notepad and types the following text in it:

```
start mspass.exe /stext mspass.txt

start mailpv.exe /stext mailpv.txt
```

Stealing Passwords Using a USB Drive 3-3

- The attacker saves this as launch.bat and copies it to the USB drive as well.
- After copying all the above the files to the USB drive, he inserts it into the USB socket of the system.
- When the autorun pop-up appears on the screen, he selects 'Perform a virus scan'.
- The files on the USB drive will start working in the background.
- Within a short span all the passwords are saved to the *.txt files on the USB drive.

Password Cracking Tools 1-5

- There are many instances when users with the strongest of passwords have fallen prey to password cracking.

- Some common password cracking tools include:

Dictionary Attack

- Can easily crack such passwords if the words in the password are mentioned in a standard dictionary.
- Scans the password for any resemblance to a word from the dictionary.

Password Cracking Tools 2-5

Brute Force Attack

- Is similar to a dictionary attack.
- Scans the password for non-dictionary words.
- Includes alpha-numeric characters such as ‘a to z’ or ‘1 to 10’.
- Though gain access to a password of a particular e-mail account, the process may vary from a couple of hours, days or even months at length.
- Is based on the complexity of the password.
- May zero down on it within an hour if a password is easy.
- Helps any systems to come up with techniques to brace themselves from brute force attacks.

Password Cracking Tools 3-5

Phishing

- Is used to acquire user details, such as username, password, debit or credit card details and so on.
- Can be done by gathering information over the phone, e-mail, social networking sites and so on.
- In case of e-mail phishing, many banks have issued circulars warning their customers to steer clear from any such e-mails and refrain from replying to the same, as banks do not demand passwords or any such vital information from their customers.

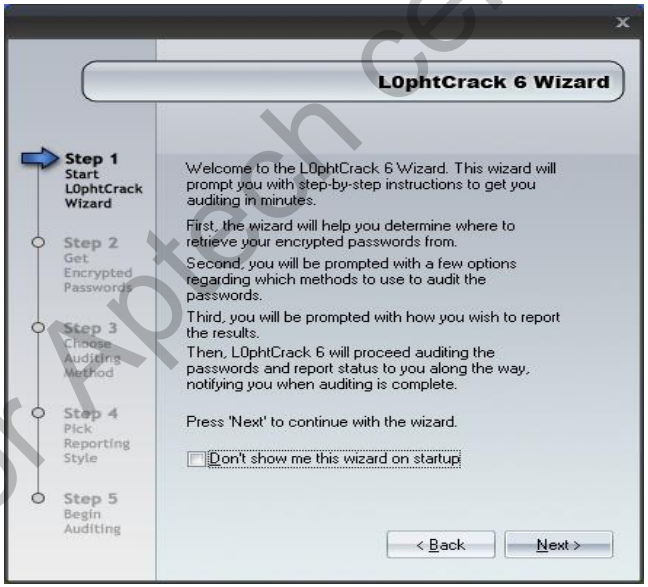
Spidering/Web Crawling

- Are programs that scout for vital data on the Web.
- Work as search engines, identifying keywords and collating them for password hacking purposes.
- Spiders are mostly used by spammers (for acquiring e-mail ids)
- Web masters (for indexing Web sites) who have to merely view the log once all the keywords are collated.

Password Cracking Tools 4-5

L0pthCrack

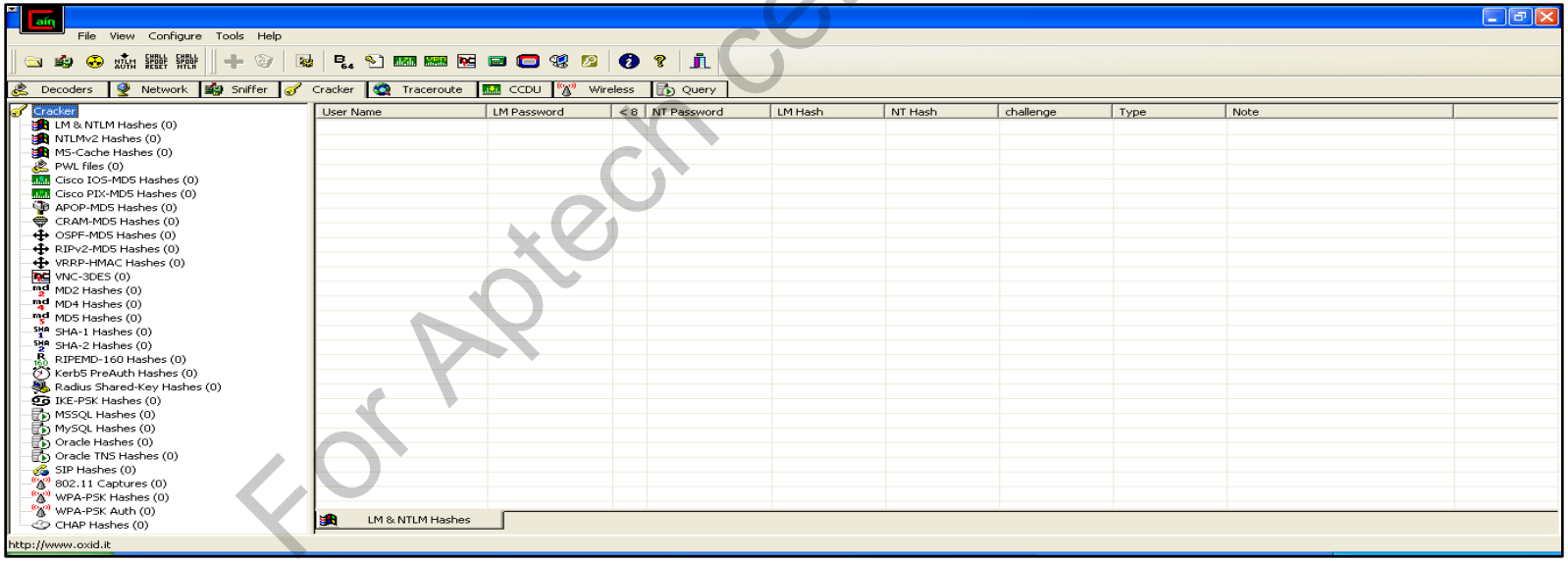
- Helps in configuring the settings needed for retrieving and auditing passwords.
- Following figure display the LophtCrack Wizard. Figure 5.34 displays the auditing process:



Password Cracking Tools 5-5

Cain and Abel

- Is a password recovery tool for the Microsoft OS.
- Allows easy recovery of various types of passwords.
- Recover the password and also covers the caching mechanisms, protocol standards and authentication methods.
- Following figure gives you an idea how Cain and Abel works.



Keyloggers 1-3

- **A Keylogger:**
  - Is software that records keystrokes made by a user.
  - Considered as spyware as well as software and stores all the keystrokes in an encrypted format into a log file saved on the computer. This data is then sent to the specified receiver.
  - Is used for surveillance by companies wanting to keep an eye on the activities of their employees.
  - Is also known to record Web site URLs in addition to keylogging keystrokes for passwords and data typed within the intranet.
  - Can be used for beneficial reasons.
  - Can also be misused and employed to transmit vital data on users to third parties.

Keyloggers 2-3

- The two types of keyloggers are:

Keylogging Software	Keylogging hardware or devices
• Comprises a *.exe file and a *.dll file. These files initiate at startup by way of a registry entry. • Are visible in the task manager, others are invisible and stealthily work in the background without leaving a trace.	• are devices fitted to the computer or the keyboard. • record each keystroke typed by the user. • This information is collated in a log file and manually retrieved or, as mentioned earlier, sent to another user through the intranet or Internet.

Keyloggers 3-3

- The following figure gives a snapshot of Spytech SpyAgent:

Spyware 1-3

- **Spyware:**

Is software that helps in garnering data about organisations or individuals without their knowledge.

Can also take over control of a computer without the user's knowledge.

- There are four types of spyware as follows:

System Monitors

Trojans

Adware

Tracking Cookies

Spyware 2-3

- Since spyware operate in the background, it is difficult to track them or even know that they are operating.
- Keylogger is a common type of spyware.
- While spyware are known to monitor the working of a computer, they also collect information over time.
- This includes Internet login passwords, e-mail ids and passwords, browser settings, software settings, vital information such as credit card or debit card account details and so on.
- Some spyware are also known to change the settings of computers, which in turn affect the Internet speeds and the operations of those computers.

Spyware 3-3

- Some valid software can sometimes be labelled as spyware due to the presence of certain *.dll files that are part of that software.
- To counter spyware attacks, a separate industry deals with the production of anti-spyware software.
- These software form a part of anti-virus software packages.
- Many jurisdictions all over the world have passed anti-spyware laws that target spyware software that are secretly installed to control a user's computer.

Rootkits

- **A Rootkit:**
  - Is a malicious software designed to hide the existence of certain processes or programs from normal methods of detection.
  - Rootkit is used to maintain control and command over a system.
  - Helps the rootkit owner or the individual who has planted it to execute the files on the system and even change configurations as per the requirement.

Covering Tracks

- **The hacker:**

Needs to ensure that he clears his tracks, no matter how much of a pro a hacker is.

Must ensure that there are no loop holes that could lead the user back to him, no matter how secure the system that was hacked was.

Why Cover Tracks?

- **Hackers cover their tracks, because**:
  - It helps them to ensure that the hacked system does not lead back to the hacker.
  - After the hack, the system can end up being vulnerable to more attacks that could further ruin the system and make it more susceptible to damage.
  - The hacker or attacker must ensure that the system works the same way it did before the hack.

Ways to Clear Online Tracks 1-3

- **To clear online tracks, the hacker:**
  - Erase all the logins and passwords generated during the hack.
  - Track down any error messages that surfaced during the hack. Usually, a log of system error messages is saved in a folder.
  - Must be aware of this and ensure that this folder is deleted after the hacking is over.
  - Must ensure that the administrator cannot apply patches to the system, change passwords or even close ports that have been opened during the hack.
  - Must remember that the administrator is his rival.
  - Should not be able to get the slightest whiff of where the attack originated from.
  - Must also ensure that the administrator does not get time to respond to the hack.
  - Identify the systems on the network that appear prone to revealing the evidence of the attack or even show any traces of the hack.
  - Erase all the traces of the hack or override it after detecting the hack.
  - Must remove any loop-hole that could lead back to him if no evidence is found.
  - Must be aware of the applications, operating systems and their versions before conducting and planning a hack.
  - Must remember that the systems will try to fight back the hacks.

Ways to Clear Online Tracks 2-3

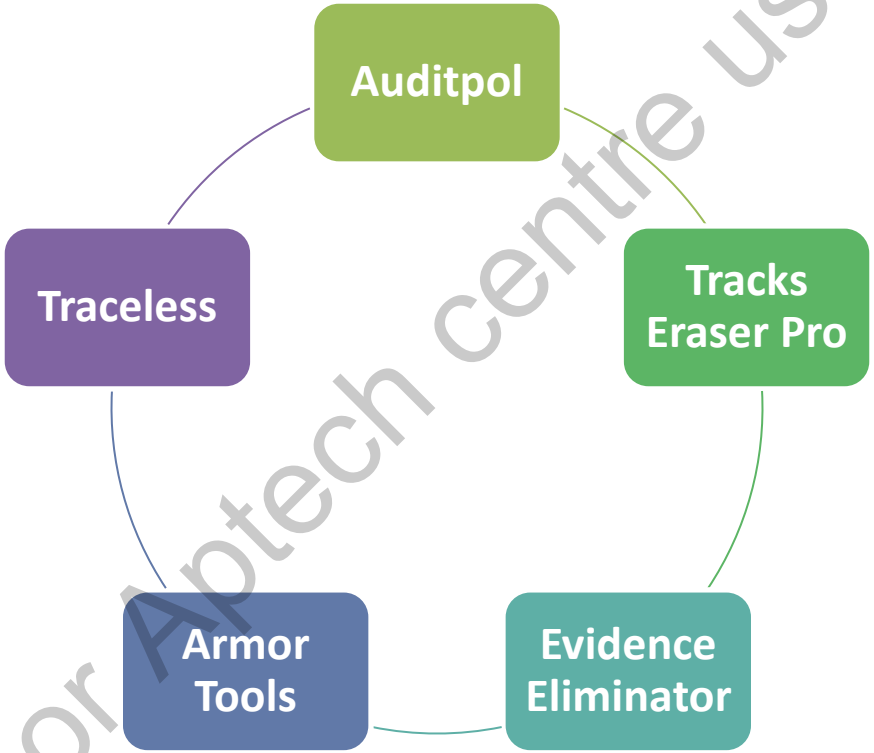
- Some common processes or applications that pose as a hindrance to hackers are firewalls, intrusion detection systems and so on.
- These processes tend to set off alarms at the slightest suspicion of an intrusion.
- Today, most antivirus software have firewalls that are built to tackle such situations.

Ways to Clear Online Tracks 3-3

- The best way of ensure that something does not get into your way is to completely bypass it.
- In case of hacking, hackers must avoid getting into the way of firewalls, honeypots and intrusion detection systems.
- These in particular are known to set off alarms during an intrusion.
- Ensure that the logs stored in the log collection systems are cleared.

Covering Tracks Tool 1-3

- Some common track covering tools include:



Covering Tracks Tool 2-3

Auditpol

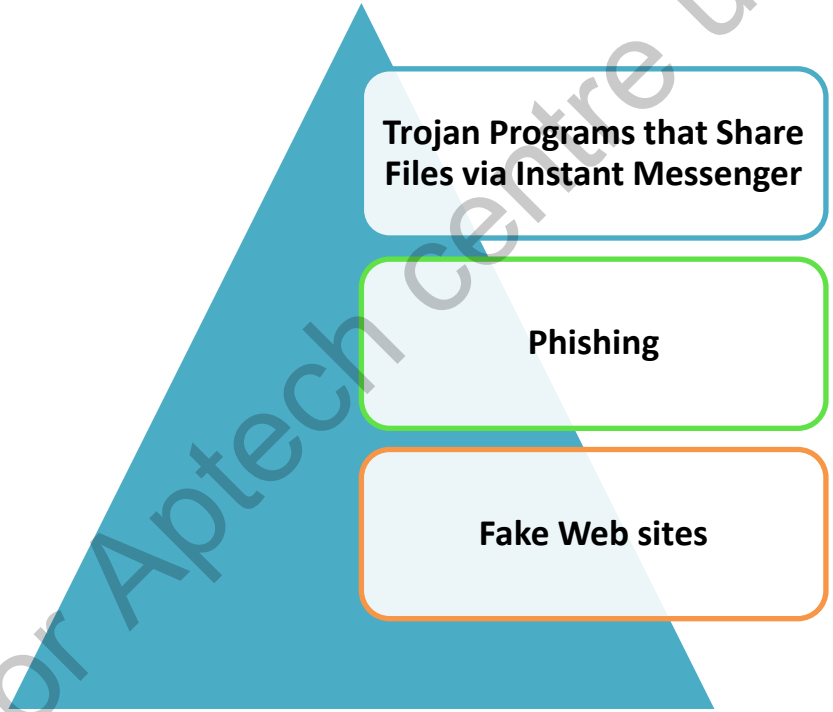
- Is an essential component of the NT resource kit
- Is used as a utility to find the target system's audit status and make changes to it.
- The following figure gives an example of the working of Auditpol:

Covering Tracks Tool 3-3

Tracks Eraser Pro	• Clears all history from the computer.
Evidence Eliminator	• Clears the history of the system by erasing files, Web site addresses, and so on.
Armor Tools	• Thwarts the saving of any activity so that there is no need to delete the log of the event.
Traceless	• Fixes Internet Explorer data.

Hacking Tricks

- The three different categories of Hacking tricks are:



Trojan Programs that Share Files via Instant Messenger 1-3

- Instant messenger allows you to share the file on a computer.
- Now days, all the instant messengers have file sharing capacity through installing patches or plug-ins.
- This could be a major threat to present information security as the messengers make it difficult to prevent information security.
- To plant Trojan programs in an unsuspected program, attackers utilise the instant communication capability.

Trojan Programs that Share Files via Instant Messenger 2-3

- These planted programs work as a hacking tool and can cover itself as it is unauthorised.
- These Trojan programs are executed without the intimation to the user and can control the computer system.
- It also read, execute, move or even delete the files in the user's computer system.

Trojan Programs that Share Files via Instant Messenger 3-3

- When the hacker replaces the installed backdoor Trojan programs that are at the remote distance with the help of instant messengers, there are certain advantages.
- For example:
  - The hacker will be informed if the victim gets online. It helps a hacker to track and access the infected computer and manipulate the information.
- A hacker can use opened instant messenger port to perform his operations.
- There is no need to open new port to perform the transmissions.

Phishing 1-5

- **In Phishing, hackers:**

Use some technical tricks to design a link of an email along with a spoofed organisation.

They use these tricks to spoof the users as a false organisation.

Phishing 2-5

- Following are the type of Phishing:

Link Manipulation

- Phishers use the misspelled URLs or sub domains. Sometimes, phishers also use the anchor text for a link appeared as a valid on the Web site, but it may lead towards the phishers' site.
- There are some old methods of spoofing such as using links that contain '@' symbol as it is the way to include the authentication credentials such as a username and password.
- These URLs or links are generally disabled in the browsers.
- The Mozilla and Opera browsers give primary warning message once user visits such links. A user can cancel the link and continue his work.
- Some problem arises when user aims to visit some international domain names and may redirect to the malicious Web site unexpectedly.
- The phishing attack takes place using some these ways to attack the important information.
- Phishers uses disguise malicious URLs with a reference of trusted domain names for their attacks.

Phishing 3-5

Filter Evasion:

- Phishers sometimes use images instead of text to avoid the scan of anti-phishing filters to detect text used in phishing emails.

Web site Forgery:

- Some phishers uses phishing scam where they use JavaScript commands to alter the address bar.
- For that, phishers place a picture of a legal URL on the address bar or close the original address bar and open a new one with the legal URL.
- An attacker sometimes creates a false script and put it in a script of a trusted Web site for the victim.
- This is known as cross-site scripting and it is tricky as it directs the user to sign in at their service's Web page.
- In reality, the link of the false service Web site is crafted to gather the private information and perform the attacks.
- It is difficult to check out these kinds of attacks as it needs specialist knowledge to identify the root of the attack.

Phishing 4-5

Phone Phishing:

- The phishing attacks are not always appears as a fake Web site.
- Sometimes the phishers send messages on the users' mobile phones claiming that the message is from bank and dial a phone number for Internet banking problems with their bank accounts details.
- Once the phishers get their log in details, they ask for account details and some more private information about the account.
- In Voice phishing, phisher uses fake caller-ID data as a bank employee and asks for account details.

Phishing 5-5

- Following are the countermeasures to be safe from the phishing:

  - Recognise phishing attempts and to deal with them.
  - Modify the browsing habits.
  - Ensure or verify the contact the company or bank when the email or a call is received for some specific information.
  - Type the company or bank Web site address and then browse the Web site instead of clicking the links in the mail.
  - Beware of suspected phishing message, mails, calls and so on.
  - Implement Anti-phishing measures in browsers as extensions Web site login procedures.

Fake Web Sites 1-3

- Following are some of the main approaches to the problem:

Identify Legitimate Sites:

- A user has to identify the authentic Web site that he aims to visit.
- For example, there are some anti-phishing toolbars that shows the domain name that user has visited.
- A user can give their pet-names as extensions for Fire-fox and type their own labels for Web sites so whenever they browse the Internet and visit the Web page, they can identify that when they have return to the site again.
- If the Web site is suspect, the anti-phishing toolbar or the software warn to the user or block the site.

Fake Web Sites 2-3

Recognise Fake Web Sites

- Hackers use the false bank Web sites to steal account credentials such as user names, passwords and account numbers as they are commonly used for online financial transactions.
- The users have to take precautions from this kind of false and tricky ways of hacking the information.
- For that, user can use secure encrypted customer's certificate and visit the site with authentic information and procedure.

Fake Web Sites 3-3

- Following are the countermeasures that help to avoid the hacker's false information, Web pages and so on:

  - Counter check the email source, address and phone number of the service organisation.
  - Check the Web site's address as the fake sites have different characters or words, names and phone numbers than the regular ones.
  - Right-click the Web site link that is received through the mail and select Properties to reveal a link's true destination.
  - Use the NO padlock in the browser window or 'https://' at the beginning of the Web address to ensure the secure link.
  - Re-assure the Web page where you have asked to enter the personal information such as user name, password and so on.

Summary 1-10

- Scanning and enumerating are the initial stages of hacking in which the hacker carries out the groundwork for system hacking.
- Ethical system hacking is conducted when the owners or users of systems provide their consent to hackers to perform this activity on their systems.
- After zeroing in on a computer or network that he or she wishes to target, the hacker then maps the computer or the network.
- Steganography is derived from the Greek word *'steganos'* meaning covered and '*graphy'* meaning writing.

Summary 2-10

- Steganography is the art of concealing the fact that communication is being carried out through media such as images, audio files, other formats such as folders, e-mails and so on.
- Steganography is the process of veiling data in hiding data within other types of data such as test files or images to communicate covert messages.
- SNOW is a program used for extracting and concealing messages in American Standard Code for Information Interchange (ASCII) text files.
- Images are commonly used for hiding data.
- In document steganography, ‘tabs’ and ‘white spaces’ are added to data.

Summary 3-10

- Video steganography involves adding a stegokey to the video file.
- The decoding of a video is to some extent the reverse of the encoding process.
- In audio steganography, audio signals are modified to transmit hidden information.
- Audio steganography relies on the psycho-acoustical masking phenomenon of the Human Auditory System (HAS).

Summary 4-10

- Some of the techniques used in audio steganography include the following:
  - Least Significant Bit (LSB): LSB coding is the simplest way of embedding information in an audio file.
  - Spread Spectrum: Spread Spectrum works on the principle that increasing the signal bandwidth in channels with narrowband noise increases the transmitted signal bandwidth.
  - Echo Hiding: In echo hiding, the secret data is concealed in the echo of the source audio.
- Audio steganography is relatively difficult to work with as compared to image steganography, as the auditory senses of human beings are stronger than their visual senses.

Summary 5-10

- In folder steganography, files are concealed in a folder.
- E-mail or spam steganography can be conducted by using the timing of the e-mail instead of its contents.
- Natural text steganography is the process of concealing data in a text-based document.
- Steganalysis is the study of identifying concealed messages using steganography. Steganalysis is often confused with cryptanalysis.
- A steganalysis attack is based on the information available to the attacker or the steganalyst.

Summary 6-10

- A steganalysis attack is based on the information available to the attacker or the steganalyst.
- Some common steganography detection tools include Stegdetect, Xstegsecret, StegSpy, Stego Watch, StegAlyzerAS, StegAlyzerRTS and StegMark.
- Password cracking is a process used for computer security. This process recovers passwords that have been stored in a computer or network.
- The two main types of password attacks employed for garnering passwords are Active online attacks and Passive online attacks.

Summary 7-10

- In passive attacks, the attacker does not contact the user or party to acquire the password.
- In active online attacks, the hacker attacks computer systems that have poor or weak passwords.
- A rainbow table is a list of hashes that have been worked out in advance.
- Distributed Network Attacks (DNA) are also known as Distributed Denial of Service (DDoS) attacks.
- Passwords can be hacked offline or in a non-electronic manner with the help of a set of hashes inserted in the password file.

Summary 8-10

- One of the most primitive and easiest ways of hacking into a system is guessing the password.
- To steal passwords offline through a USB drive, all the hacker has to do is copy password hacking software, such as messenPass or MailPassView, on a USB drive of 1 GB capacity or more.
- There are many instances when, despite the strongest passwords, users have fallen prey to password cracking.
- A keylogger is software that records keystrokes made by a user.

Summary 9-10

- A spyware as well as software, keylogger stores all the keystrokes in an encrypted format to a log file saved on the computer.
- Spyware is software that helps in garnering data about organisations or individuals without their knowledge.
- A rootkit is a malicious software designed to hide the existence of certain processes or programs from normal methods of detection.
- It is important to cover ones tracks after a hack to ensure that the hacked system does not lead back to the hacker.
- Every hacker must be aware of the applications, operating systems and their versions before conducting a hack.

Summary 10-10

- **Some common track covering tools are as follows:**
  - Auditpol: An essential component of the NT resource kit, this tool is used to find and audit
  - Tracks Eraser Pro: This tool clears all history from the computer.
  - Evidence Eliminator: This tool clears the history of the system by erasing files, Web site addresses and so on.
  - Armor Tools: This tool thwarts the saving of any activity so that there is no need to delete the log of the event.
  - Traceless: This tool fixes Internet Explorer data.