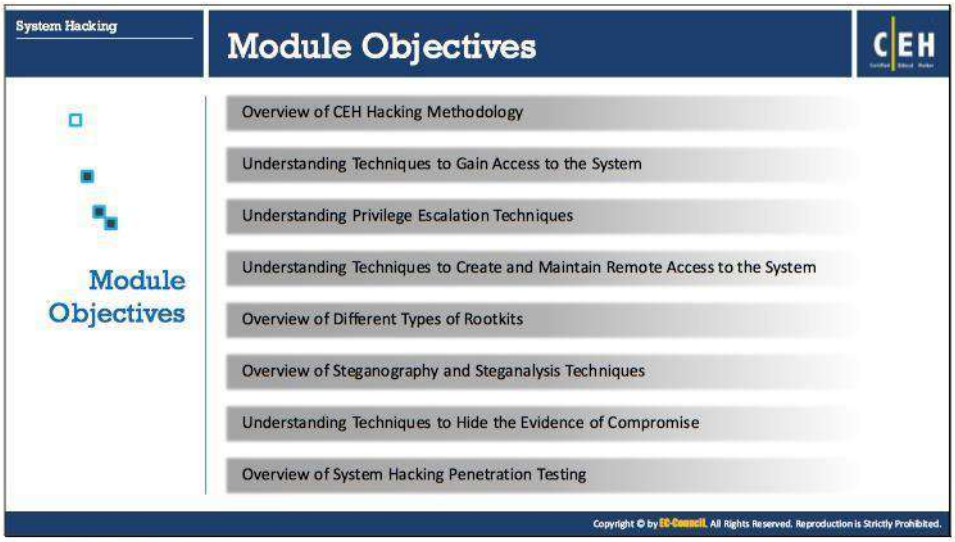
C|EH
Certified Ethical Hacker

Module 06

System Hacking

This page is intentionally left blank.



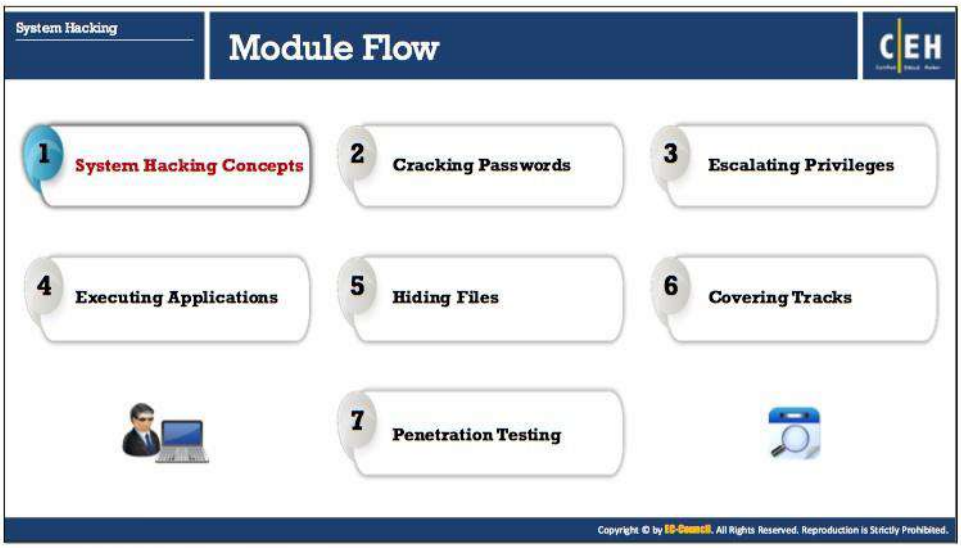
Module Objectives

System hacking is one of the most important and, sometimes, the ultimate goal of an attacker. The attacker acquires information through techniques such as footprinting, scanning, and enumeration, and uses it to hack the target system. This module will focus your awareness on the tools and techniques used by the attacker to achieve his/her goal of hacking the target system.

This module starts with an overview of hacking methodology. Later, it discusses in detail various hacking stages, such as gaining and maintaining access, and clearing logs. The module ends with a discussion on system hacking penetration testing.

At the end of this module, you will be able to:

- Describe the CEH Hacking Methodology
- Explain different techniques to gain access to the system
- Apply privilege escalation techniques
- Explain different techniques to create and maintain remote access to the system
- Describe different types of rootkits
- Explain steganography and steganalysis techniques
- Apply different techniques to hide the evidence of compromise
- Perform system hacking penetration testing



System Hacking Concepts

An attacker engages in system hacking attempts using information collected in earlier footprinting, scanning, enumeration, and vulnerability analysis phases. Let us go over these phases and the information collected thus far.

Prior to this module, we discussed:

- **Footprinting Module:** Footprinting is the process of accumulating data regarding a specific network environment. In the footprinting phase, the attacker creates a profile of the target organization, obtaining information such as its IP address range, namespace, and employees.

  Footprinting eases the process of system hacking by revealing its vulnerabilities. For example, the organization's website may provide employee bios or a personnel directory, which the hacker can use it for social engineering purposes. Conducting a Whois query on the web can provide information about the associated networks and domain names related to a specific organization.

- **Scanning Module:** Scanning is a procedure for identifying active hosts, open ports, and unnecessary services enabled on particular hosts. Attackers use different types of scanning, such as port scanning, network scanning, and vulnerability scanning of target networks or systems, which help in identifying possible vulnerabilities. Scanning procedures such as port scanning and ping sweep return information about the services offered by the live hosts that are active on the Internet, and their IP addresses.

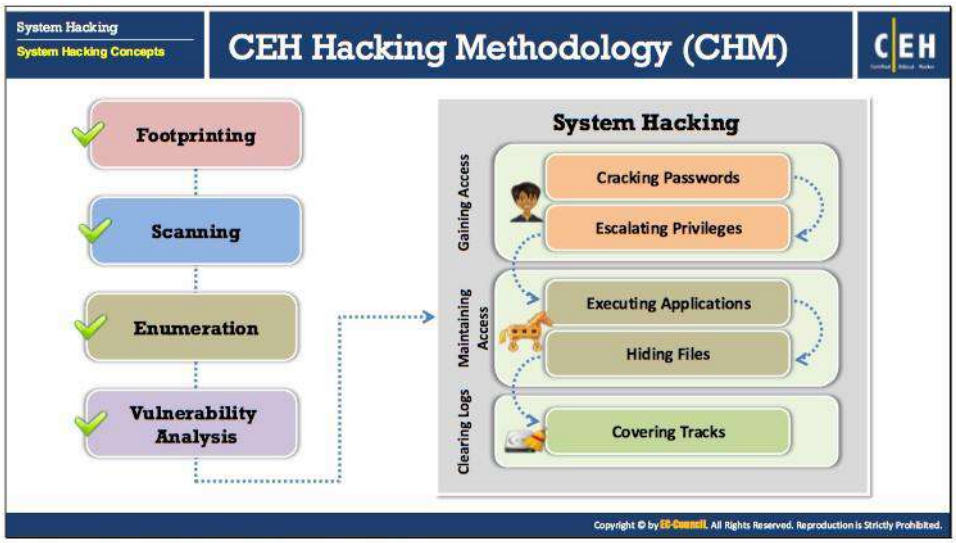
- **Enumeration Module:** Enumeration is a method of intrusive probing, through which attackers gather information such as network user lists, routing tables, security flaws, and Simple Network Management Protocol (SNMP) data. This is significant, because the

attacker ranges over the target territory to glean information about the network, and shared users, groups, applications, and banners.

Enumeration involves making active connections to the target system or subjecting it to direct queries. Normally, an alert and secure system will log such attempts. Often, the information gathered is publicly available anyway, such as a DNS address; however, it is possible that the attacker might stumble upon a remote IPC share, such as IPC$ in Windows, that can be probed with a null session, thus allowing shares and accounts to be enumerated.

- **Vulnerability Analysis Module:** Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels

  Attackers perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. The identified vulnerabilities are used by the attackers to perform further exploitation on that target network.



CEH Hacking Methodology (CHM)

In preparation for hacking a system, attackers follow a certain methodology. They first obtain information during the footprinting, scanning, and enumeration phases, which they then use to exploit the target system. There are three steps in the CEH Hacking Methodology (CHM):

- **Gaining Access**

  Involves gaining access to low-privileged user accounts by cracking passwords through techniques such as brute-forcing, password guessing, and social engineering, and then escalating their privileges to administrative levels, to perform a protected operation.

- **Maintaining Access**

  After successfully gaining access to the target system, attackers work to maintain high levels of access to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files.

- **Clearing Logs**

  To maintain future system access, attackers attempt to avoid recognition by legitimate system users. To remain undetected, attackers wipe out the entries corresponding to their activities in the system log, thus avoiding detection by users.

System Hacking Goals

The intent of every criminal is to achieve a certain goal. Likewise, attackers can have certain goals behind their system attacks. The following are some goals of system attackers. The diagram in the slide shows these goals at different hacking stages and the techniques used to achieve them.

- **Gaining Access**

  In system hacking, the attacker first tries to gain access to a target system using information obtained and loopholes found in the system's access control mechanism. Once attackers succeed in gaining access to the system, they are free to perform malicious activities such as stealing sensitive data, implementing a sniffer to capture network traffic, and infecting the system with malware. At this stage, attackers use techniques such as password cracking and social engineering tactics to gain access to the target system.

- **Escalating Privileges**

  After gaining access to a system using a low-privileged normal user account, attackers may then try to increase their administrator privileges to perform protected system operations, so that they can proceed to the next level of the system hacking phase: to execute applications. Attackers exploit known system vulnerabilities to escalate user privileges.

- **Executing Applications**

  Once attackers have administrator privileges, they attempt to install malicious programs such as Trojans, Backdoors, Rootkits, and Keyloggers, which grant them remote system access, thereby enabling them to execute malicious codes remotely. Installing Rootkits

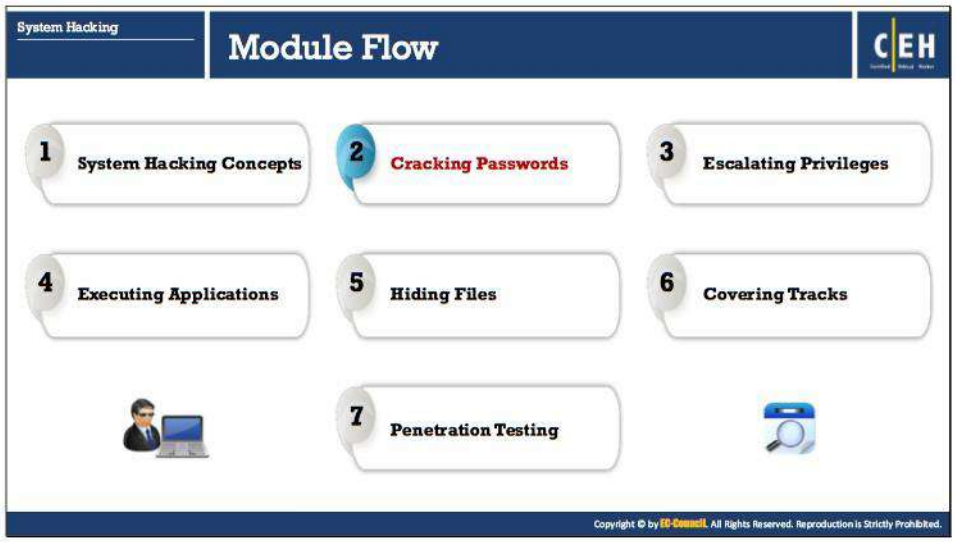
allows them to gain access at the operating system level to perform malicious activities. To maintain access for use at a later date, they may install Backdoors.

- **Hiding Files**

  Attackers use Rootkits and steganography techniques to attempt to hide the malicious files they install on the system, and thus their activities.

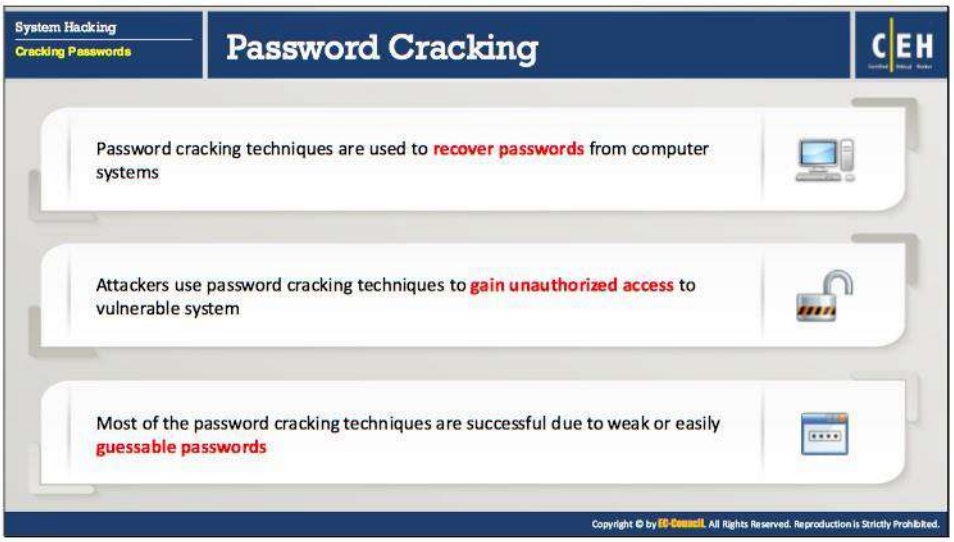
- **Covering Tracks**

  To remain undetected, it is important for attackers to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.



Cracking Passwords

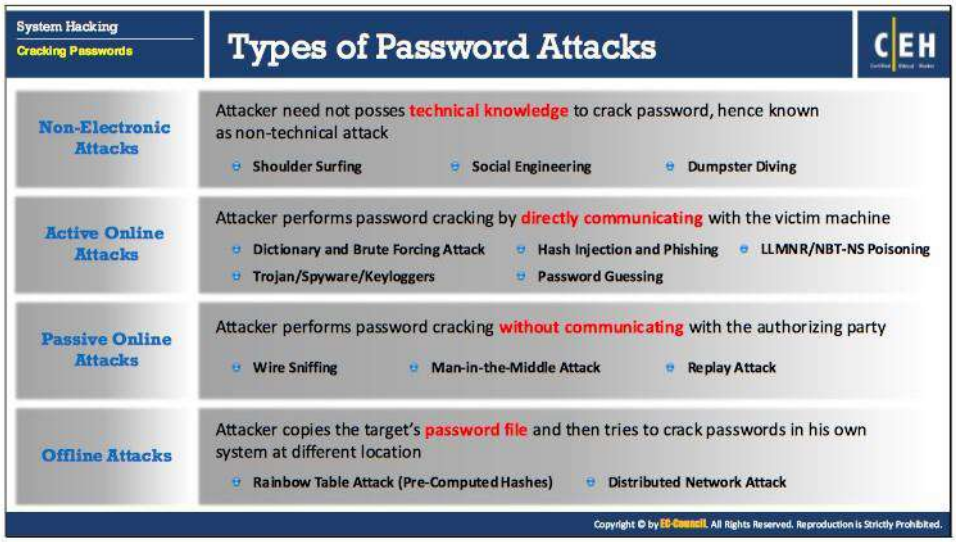
As discussed earlier, CHM involves various steps attackers follow to hack systems. The following section discusses these steps in greater detail. The first step, password cracking, discusses different tools and techniques attackers use to crack password on the target system.



Password Cracking

Password cracking is the process of recovering passwords from the data transmitted by a computer system or stored in it. The purpose of password cracking might be to help a user recover a forgotten or lost password, as a preventive measure by system administrators to check for easily breakable passwords, or an attacker can use this process to gain unauthorized system access.

Hacking often begins with password cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it, or use automated tools and techniques such as a dictionary or a brute-force method. Most password cracking techniques are successful because of weak or easily guessable passwords.



Types of Password Attacks

Password cracking is one of the crucial stages of system hacking. Password cracking mechanisms often exploit otherwise legal means to gain unauthorized system access, such as recovering a user's forgotten password. Classification of password attacks depends on attackers' actions, which are typically one of four types:

- **Non-Electronic Attacks:** This is probably the attacker's first attempt at gaining target system passwords. Non-electronic or non-technical attacks do not require any technical knowledge about hacking or system exploitation. Therefore, this is a non-electronic attack. Techniques used to perform non-electronic attacks include shoulder surfing, social engineering, dumpster diving, etc.
- **Active Online Attacks:** This is one of the easiest ways to gain unauthorized administrator-level system access. An attacker needs to communicate with target machines to gain password access. Techniques used by the attacker to perform active online attacks include password guessing, dictionary and brute forcing attack, hash injection, phishing, LLMNR/NBT-NS Poisoning, using Trojan/spyware/keyloggers, etc.
- **Passive Online Attacks:** A passive attack is a system attack that does not result in a change to the system in any way. In this attack, the attacker does not need to communicate with the system. Instead, he/she passively monitors or records the data passing over the communication channel to and from the system. The attacker then uses the observed data to break into the system. Techniques used to perform passive online attacks include wire sniffing, man-in-the-middle attack, replay attack, etc.

- **Offline Attacks:** Offline attack refers to password attacks where an attacker tries to recover clear text passwords from a password hash dump. Offline attacks are often time consuming, but can be successful, as password hashes can be reversed due to their smaller keyspace and shorter length. Attackers use pre-computed hashes from rainbow tables to perform offline and distributed network attack.

Non-Electronic Attacks

Non-electronic, or non-technical, attacks do not require technical knowledge of methods of system intrusion. There are four types of non-electronic attacks: social engineering, shoulder surfing, keyboard sniffing, and dumpster diving.

- **Dumpster Diving**

  "Dumpster diving" is a key attack method that targets a substantial failure in computer security. The sensitive information that people crave, protect, and devotedly secure can be accessed by almost anyone willing to scrutinize garbage. Looking through the trash is a type of low-tech attack with many implications.

  Dumpster diving was actually quite popular in the 1980s. The term itself refers to the collection of any useful, general information from waste dumps such as trashcans, curbside containers, and dumpsters. Even today, curious and/or malicious attackers sometimes find discarded media with password files, manuals, reports, receipts, credit card numbers, or other sensitive documents.

  Examination of waste products from waste dumps can help attackers, and there is ample evidence to support this concept. Support staff often dumps sensitive information without a thought regarding as to whose hands it may end up in. Attackers thus gain unauthorized system access using these methods. Likewise, the objects found can lead to other types of attacks, such as social engineering.

- **Shoulder Surfing**

  Shoulder surfing is a technique through which attackers steal passwords by hovering near legitimate users and watching them enter their passwords. Attackers simply watch users' keyboards or screens as they log in, and to see if users refer to, for example, an

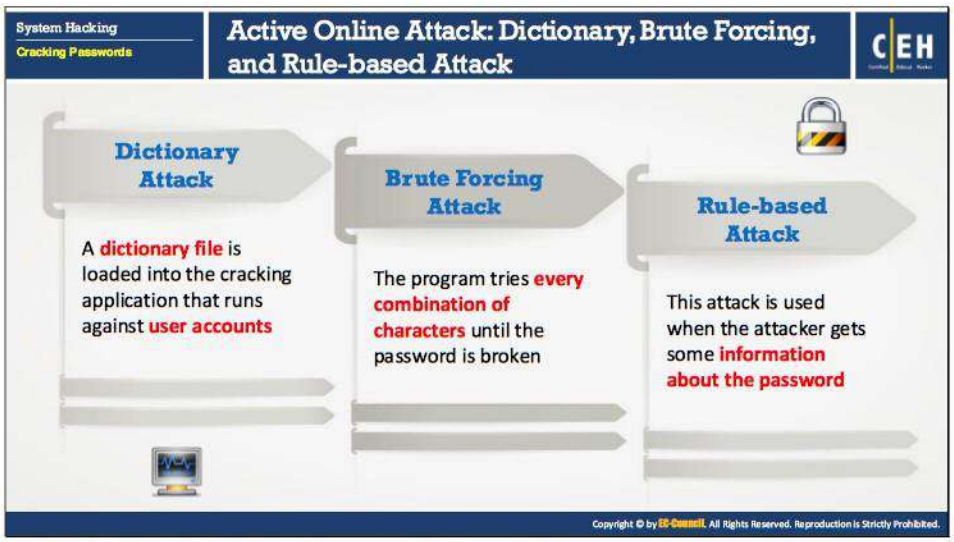
object on their desks for written passwords or mnemonics. Obviously, shoulder surfing is possible only in some proximity to the target.

This type of attack can also occur in a grocery store checkout line, when a potential victim is swiping a debit card and entering the required PIN (Personal Identification Number), which is typically only four digits, making it easier to observe.

- **Social Engineering**

  In computer security, social engineering is the term applied to a non-technical type of intrusion that exploits human behavior. Typically, it relies heavily on human interaction and often involves tricking other people into breaking normal security procedures. A social engineer runs a "con game" to break security procedures. For example, an attacker using social engineering to break into a computer network would try to gain the trust of someone authorized to access the network, and then try to extract the information that compromises network security. Social engineering is, in effect, a run-through used to procure confidential information by deceiving or swaying people. An attacker can misrepresent himself/herself as a user or system administrator to obtain a user's password. It is natural for people to be helpful and trusting. People generally make an effort to build amicable relationships with friends and colleagues. Social engineers take advantage of this tendency.

  Another trait of social engineering relies on the inability of people to keep up with a culture that relies heavily on information technology. Most people are not aware of the value of the information they possess and few are careful about protecting it. Attackers take advantage of this fact. Social engineers will typically search dumpsters for valuable information. A social engineer would have a tougher time getting the combination to a safe, or to a health-club locker, than a password. The best defense is to educate, train, and create awareness.



Active Online Attack: Dictionary, Brute Forcing, and Rule-based Attack

- **Dictionary Attack**

  In a dictionary attack, a dictionary file is loaded into the cracking application that runs against user accounts. This dictionary is the text file that contains a number of dictionary words that are commonly used as passwords. The program uses every word present in the dictionary to find the password. Apart from a standard dictionary, attackers' dictionaries have added entries with numbers and symbols added to words (e.g., "3December!962"). Simple keyboard finger rolls ("qwer0987"), which many believe to produce random and secure passwords, are thus included in an attacker's dictionary. Dictionary attacks are more useful than brute force attacks. However, dictionary attacks do not work in systems using passphrases.

  This attack is applicable under two situations:

  - In cryptanalysis, to discover the decryption key for obtaining the plaintext from ciphertext
  - In computer security, to bypass authentication and access control mechanism of the computer by guessing passwords

  Methods to improve the success of a dictionary attack:

  - Use of a number of different dictionaries, such as Technical and foreign dictionaries, which increases the number of possibilities
  - Use of string manipulation with the dictionary (e.g., if the dictionary contains the word "system," string manipulation creates anagrams like "metsys," among others)

- **Brute-Force Attack**

  In a brute force attack, attackers try every combination of characters until the password is broken. Cryptographic algorithms must be sufficiently hardened to prevent a brute-force attack, which is defined by the RSA: "Exhaustive key-search, or brute-force search, is the basic technique for trying every possible key in turn until the correct key is identified."

  Brute-force attack is when someone tries to produce each single encryption key for data to detect the needed information. Even today, only those with sufficient processing power could successfully perform this type of attack.

  Cryptanalysis is a brute-force attack on an encryption employing a search of the keyspace. In other words, testing all possible keys is one of the attempts to recover the plaintext used to produce a particular ciphertext. The detection of a key or plaintext that is faster than a brute force attack is one way of breaking the cipher. A cipher is secure if no method exists to break it other than a brute-force attack. Mostly, all ciphers are deficient in mathematical proof of security. If the user chooses keys randomly or searches randomly, the plaintext will become available after the system tries half of all the possible keys.

  Some of the considerations for brute-force attacks are:

  - It is a time-consuming process.
  - All passwords will eventually be found.

- **Rule-based Attack**

  Attackers use this type of attack when they obtain some information about the password. This is a more powerful attack than the dictionary and brute-force attacks, because the cracker knows the password type. For example, if the attacker knows that the password contains a two- or three-digit number, he or she will use some specific techniques to extract the password quickly.

  By obtaining useful information such as the method in which numbers and/or special characters have been used, and password length, attackers can minimize the time required to crack the password and thereby enhance the cracking tool. This technique involves brute force, a dictionary, and syllable attacks.

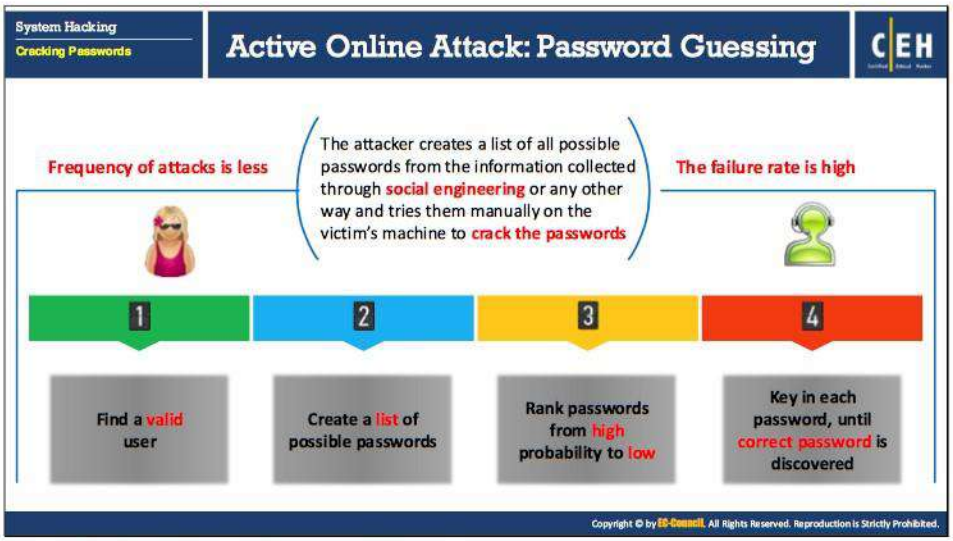
  For online password cracking attacks, an attacker will sometimes use a combination of both brute force and a dictionary. This combination falls into the category of Hybrid and Syllable password cracking attacks.

  - **Hybrid Attack**

    This type of attack depends on the dictionary attack. Often, people change their passwords merely by adding some numbers to their old passwords. In this case, the program would add some numbers and symbols to the words from the dictionary to try and crack the password. For example, if the old password is "system," then there is a chance that the person will change it to "system1" or "system2."

- **Syllable Attack**

  Hackers use this cracking technique when passwords are not known words. Attackers use the dictionary and other methods to crack them, as well as all possible combinations of them.



Active Online Attack: Password Guessing

Password guessing is one of the password cracking techniques that involves attempting to log on to the target system with different passwords manually. Guessing is the key element of manual password cracking. The attacker creates a list of all possible passwords from the information collected through social engineering or any other way and tries them manually on the victim's machine to crack the passwords.

The following are the steps involved in password guessing:

- Find a valid user
- Create a list of possible passwords
- Rank passwords from high probability to low
- Key in each password, until correct password is discovered

Hackers can crack the passwords manually or by using automated tools, methods, and algorithms. They can also automate password cracking using a simple FOR loop. A hacker can also create a script file that tries each password in a list. Still, these techniques are considered manual cracking. The failure rate of this type of attack is high.

Manual Password-Cracking Algorithm

In its simplest form, this algorithm can automate password guessing using a simple FOR loop. In the example that follows, an attacker creates a simple text file with user names and passwords and iterates them using the FOR loop.

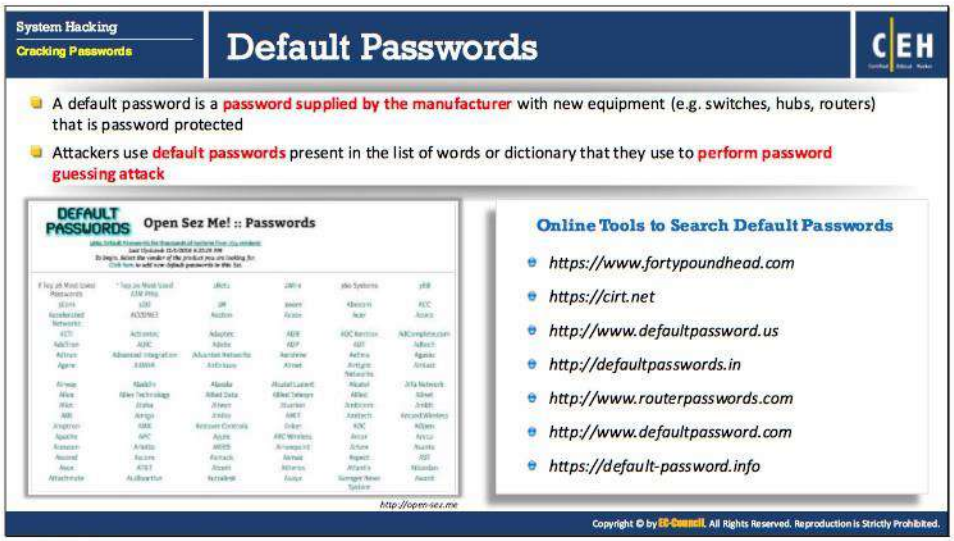
The main FOR loop can extract the user names and passwords from the text file, which serves as a dictionary as it iterates through every line:

```
[file: credentials.txt]
administrator ""
administrator password
administrator administrator
[Etc.]
```

Type the following commands to access the text file from a directory:

```
c:\>FOR /F "tokens=1,2*" %i in (credentials.txt)^
More? do net use \\victim.com\IPC$ %j /u:victim.com\%i^
More? 2>>nul^
More? && echo %time% %date% >> outfile.txt^
More? && echo \\victim.com acct: %i pass: %j >> outfile.txt
c:\>type outfile.txt
```

The outfile.txt contains the correct user name and password, if the user name and password in credentials.txt are correct. An attacker can establish open session with the victim server using his/her system.

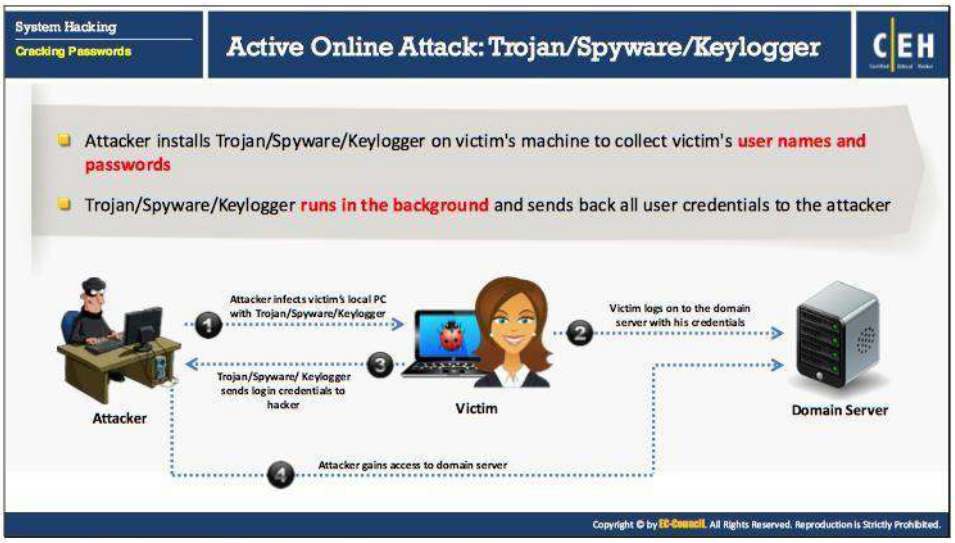


Default Passwords

Default passwords are those supplied by manufacturers with new equipment (e.g. switches, hubs, routers). Usually, default passwords provided by the manufacturers of password-protected devices allow the user to access the device during initial setup, and then change the password. But often, an administrator will either forget to set the new password or ignore the password-change recommendation and continue using the original password. Attackers can exploit this lapse and find the default password for the target device from manufacturer websites or using online tools which shows default passwords to successfully access the target device. Attackers use default passwords in the list of words or dictionary that they use to perform password guessing attack.

The following are some of the online tools to search default passwords:

- *http://open-sez.me*
- *https://www.fortypoundhead.com*
- *https://cirt.net*
- *http://www.defaultpassword.us*
- *http://defaultpasswords.in*
- *http://www.routerpasswords.com*
- *http://www.defaultpassword.com*
- *https://default-password.info*



Active Online Attack: Trojan/Spyware/Keylogger

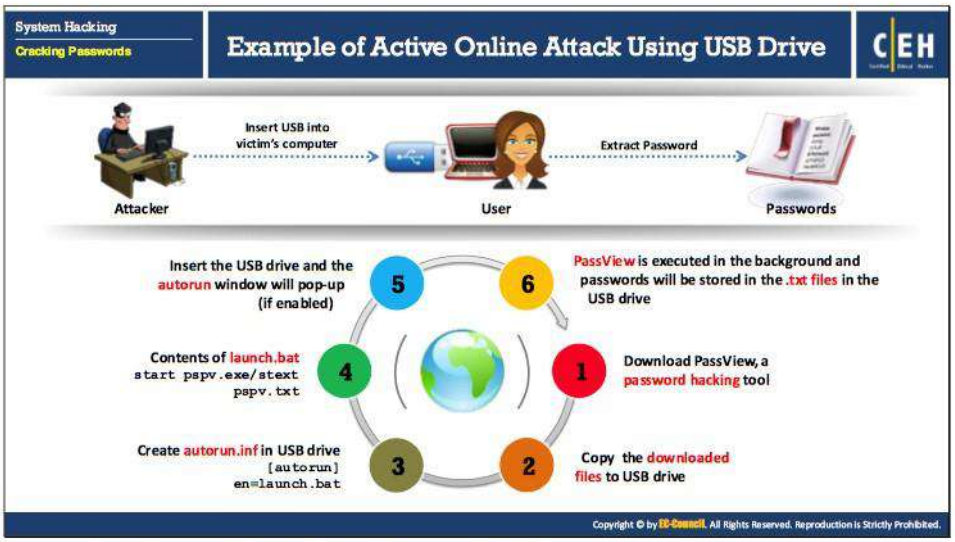
A Trojan is a program that masks itself as a benign application. The software initially appears to perform a desirable or benign function but instead steals information or harms the system. With a Trojan, attackers can gain remote access and perform various operations limited by user privileges on the target computer.

Spyware is a type of malware that attackers install on a computer to secretly gather information about its users without their knowledge. Spyware hides itself from the user and can be difficult to detect.

A keylogger is a program that records all user keystrokes without the user's knowledge. Keyloggers ship the log of user keystrokes to an attacker machine or hide it in the victim's machine for later retrieval. The attacker then scrutinizes them carefully for finding passwords or other useful information that could compromise the system.

An attacker installs Trojan/Spyware/Keylogger on a victim's machine to collect the victim's user names and passwords. These programs run in the background and send back all user credentials to the attacker.

For example, a key logger on a victim's computer is capable of revealing the contents of all user emails. The picture given in the slide depicts a scenario describing how an attacker gains password access using a Trojan/Spyware/Keylogger.



Example of Active Online Attack Using USB Drive

Obtaining passwords using a USB drive is a physical approach for password hacking. Attackers can steal passwords using a USB drive and different applications. People who have multiple online accounts usually store their user names and passwords as a backup in case they forget them. You can recover or steal such credentials using a USB drive.

The physical approach matters a lot for hacking passwords. One can steal passwords using a USB drive and applications. This method is applicable for hacking stored passwords on any computer. Most of the people signing up for a large number of websites usually store their passwords on the computer to remember them. Recovering passwords automatically using a USB drive requires plugging the USB drive in any port of the target computer. This trick is applicable for Windows XP, Windows 2000, Windows Vista, and Windows 7.

All the applications included are portable and light enough to download to the USB drive in seconds. You can also hack stored Messenger passwords. Using tools and a USB pen drive, you can create a rootkit to hack passwords from the target computer.

Following are the steps to steal passwords using a USB device:

1. You need to download PassView, a password hacking tool.
2. Copy the downloaded .exe PassView file to the USB drive.
3. Create a Notepad document, and put the following content or code in the notepad:

   [autorun]

   en=launch.bat

After writing this content into Notepad, save the document as autorun.inf and copy this file to the USB drive.

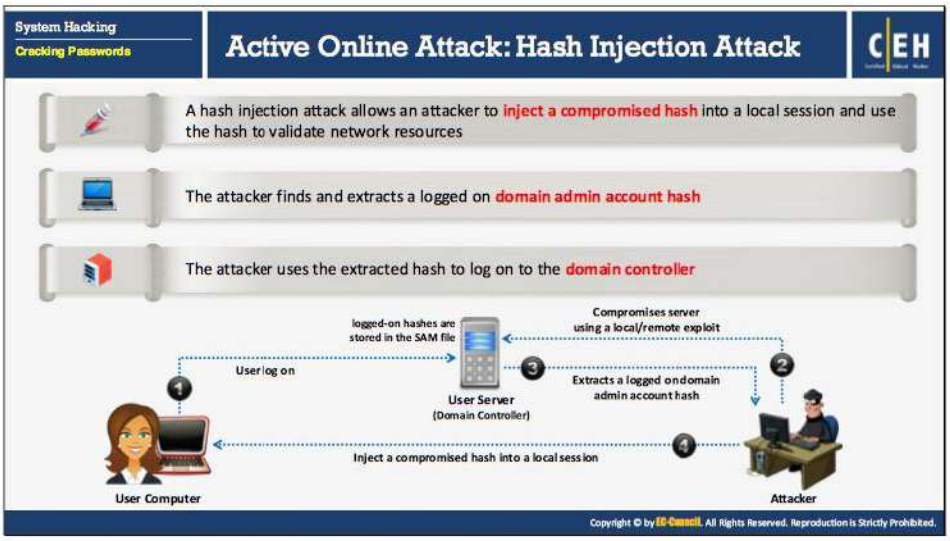
4. Open Notepad, and write the following content:

   start pspv.exe/stext pspv.txt

   After that, save file as launch.bat and copy this file to the USB drive.

5. Insert the USB drive and the autorun window pop-up appears (if enabled).
6. PassView (or other password-hacking tool) runs in the background and stores the passwords in the .txt files on the USB drive.

In this way, you can create your own USB password recovery toolkit and use it to steal the stored passwords of your friends or colleagues without their knowledge. It only takes a few seconds to retrieve passwords.



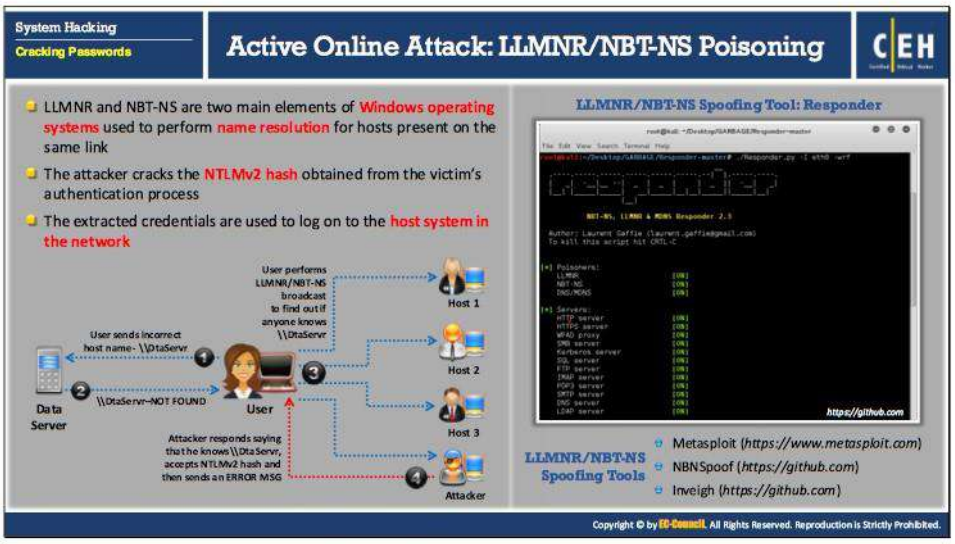
Active Online Attack: Hash Injection Attack

This type of attack is possible when the target system uses a hash function as part of the authentication process to authenticate its users. Generally, the system stores hash values of the credentials in the SAM database/file on a Windows computer. In such cases, the server computes the hash value of the user-submitted credentials or allows user to input the hash value directly. The server then checks it against the stored hash value for authentication.

Attackers take advantage of such authentication mechanisms and first exploit the target server to retrieve the hashes from the SAM databases. They then input the hashes acquired directly into the authentication mechanism to authenticate with stolen user's pre-computed hashes. Thus, in a hash injection attack, the attackers inject a compromised hash into a local session and then use the hash to authenticate to the network resources.

The hacker carries out this attack by implementing the following four steps:

- The hacker compromises one workstation/server using a local/remote exploit.
- The hacker extracts stored hashes and finds a domain admin account hash.
- The hacker uses the hash to log on to any system (domain controller) with the same credentials.
- The hacker extracts all the hashes from the Active Directory database and can now compromise any account in the domain.



Active Online Attack: LLMNR/NBT-NS Poisoning

LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows operating systems used in order to perform name resolution for hosts present on the same link. These services are enabled by default in Windows operating systems.

When the DNS server fails in an attempt to resolve name queries, the host performs an unauthenticated UDP broadcast asking all the hosts if anyone has a name that it is looking for. Due to the fact that the host trying to connect is following an unauthenticated and broadcast process, it becomes easy for an attacker to passively listen to a network for LLMNR (UDP port 5355) and NBT-NS (UDP port 137) broadcasts, and respond to the request pretending to be a target host. After accepting a connection with a host, the attacker can make use of tools such as Responder.py or Metasploit to forward the request to a rogue server (For instance TCP: 137) to perform an authentication process.

During the authentication process the attacker sends an NTLMv2 hash to the rogue server which was obtained from the host trying to authenticate itself. This hash is stored in a disk and can be cracked using offline hash cracking tools such as hashcat or John the ripper. Once cracked, those credentials can be used to log in to get an access to the legitimate host system.

Steps involved in LLMNR/NBT-NS poisoning:

1. User sends a request to connect to the data sharing system, \\DataServer which she mistakenly typed as \\DtaServr.
2. The \\DataServer responds to the user saying that it does not know the host named \\DtaServr.
3. The user then performs LLMNR/NBT-NS broadcast to find out if anyone in the network knows the host name\\DtaServr.
4. The attacker replies to the user saying that it is \\DataServer and accepts user NTLMv2 hash and responds to the user with an error.

LLMNR/NBT-NS Poisoning Tools

- **Responder**

  Source: *https://github.com*

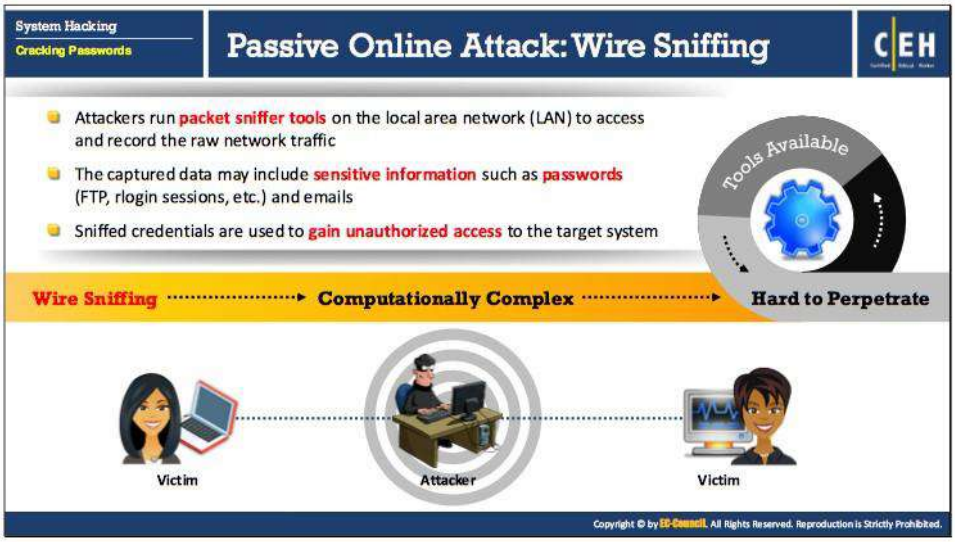
  Responder an LLMNR, NBT-NS and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

  Features:

  - Built-in SMB Auth server, MSSQL Auth server, HTTP and HTTPs Auth server, HTTPS Auth server, LDAP Auth server
  - Built-in FTP, POP3, IMAP, SMTP Auth servers
  - ICMP Redirect
  - Rogue DHCP

Some of the LLMNR/NBT-NS spoofing tools are listed below:

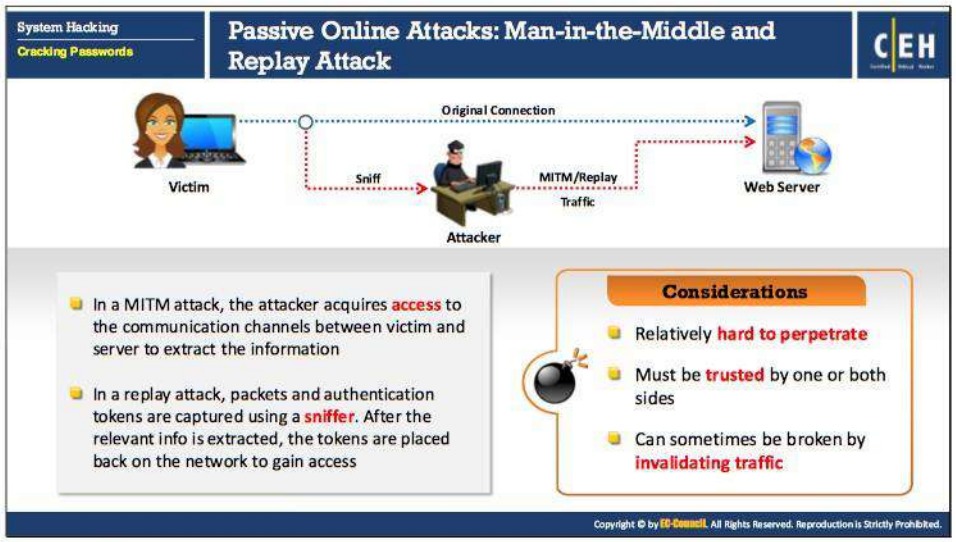
- Metasploit (*https://www.metasploit.com*)
- NBNSpoof (*https://github.com*)
- Inveigh (*https://github.com*)



Passive Online Attack: Wire Sniffing

Packet sniffing is a form of wire sniffing or wiretapping in which hackers sniff credentials during transit by capturing Internet packets. Attackers rarely use sniffers to carry out this type of attack. With packet sniffing, an attacker can gain passwords such as Email, websites, SMB, FTP, rlogin sessions or SQL. As sniffers run in the background, the victim will not be aware of the sniffing.

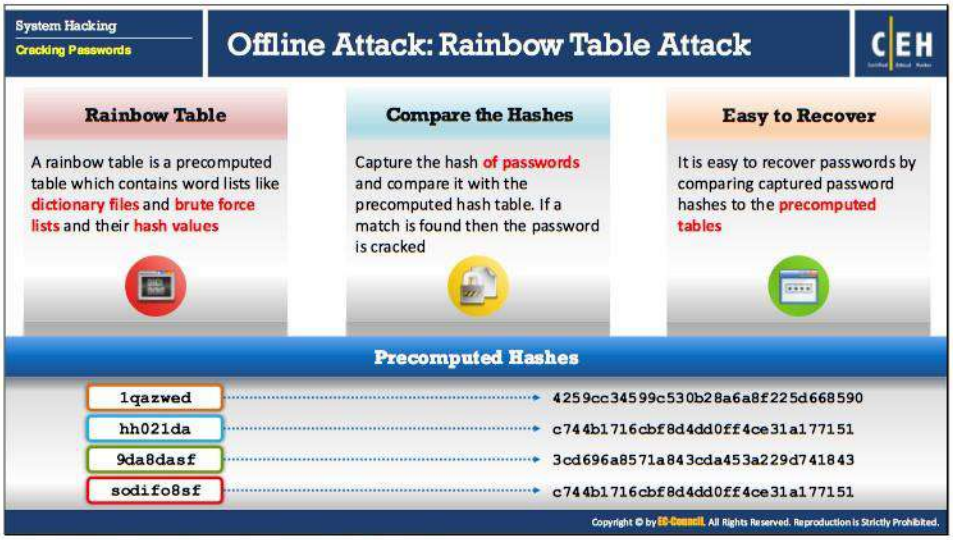
As sniffers gather packets at the Data Link Layer, they can grab all the packets on the LAN of the machine running the sniffer program. This method is relatively hard to perpetrate and is computationally complicated. This is because a network with a hub implements a broadcast medium that all systems share on the LAN. The LAN sends the data to all machines connected to it. If an attacker runs a sniffer on one system on the LAN, he or she can gather data sent to and from any other system on the LAN. The majority of sniffer tools are ideally suited to sniff data in a hub environment. These tools are passive sniffers, as they passively wait for data transfer before capturing the information. They are efficient at imperceptibly gathering data from the LAN. The captured data may include passwords sent to remote systems during FTP, rlogin sessions, and electronic mail. The attacker uses these sniffed credentials to gain unauthorized access to the target system. There are a variety of tools available on the Internet for passive wire sniffing.



Passive Online Attacks: Man-in-the-Middle and Replay Attack

When two parties are communicating, a man-in-middle attack can take place, in which a third party intercepts a communication between the two parties without their knowledge. Meanwhile, the third party eavesdrops on the traffic, and then passes it along. To do so, the "man in the middle" has to sniff from both sides of the connection simultaneously. In a MITM attack, the attacker acquires access to the communication channels between victim and server to extract the information. This type of attack is often used in telnet and wireless technologies. It is not easy to implement such attacks because of the TCP sequence numbers and the speed of the communication. This method is relatively hard to perpetrate and can sometimes be broken by invalidating the traffic.

In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access. The attacker uses this type of attack to replay bank transactions or other similar types of data transfer, in the hope of replicating and/or altering activities, such as banking deposits or transfers.



Offline Attack: Rainbow Table Attack

Offline attacks occur when the intruder checks the validity of passwords. She/he observes how the password is stored. If the user names and passwords are stored in a file that is readable, it becomes easy for the attacker to gain access to the system. Hence, it is important to protect the passwords list and keep it in an unreadable form, preferably encrypted.

Offline attacks are time consuming. However, they can be successful due to their smaller keyspace and shorter length. Different password cracking techniques are available on the Internet.

Two examples of offline attacks are:

1. Rainbow Table Attack
2. Distributed Network Attack

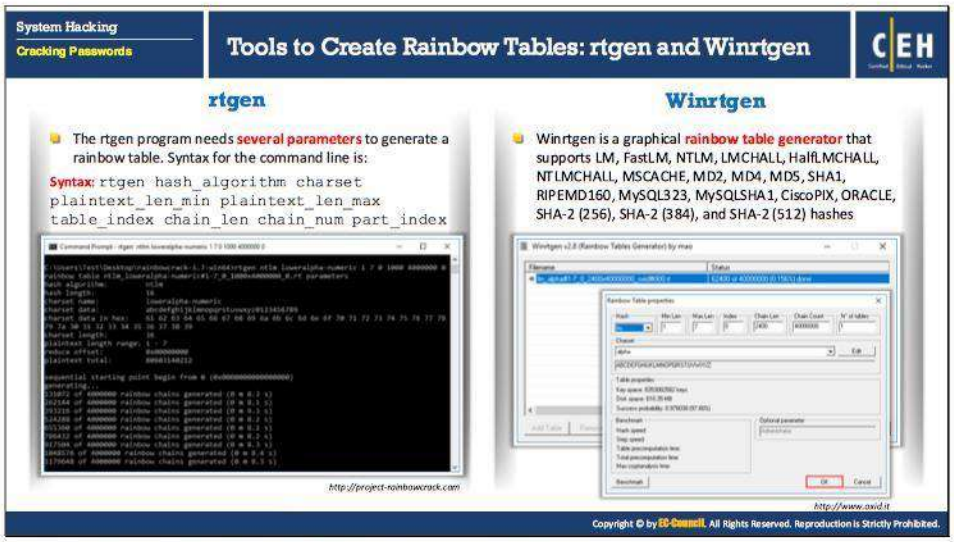
Rainbow Table Attack

A rainbow table attack uses the cryptanalytic time-memory trade-off technique, which requires less time than some other techniques. It uses already-calculated information stored in memory to crack the cryptography. In the rainbow table attack, the attacker creates a table of all the possible passwords and their respective hash values, known as a rainbow table, in advance.

Rainbow Table: A rainbow table is a precomputed table which contains word lists like dictionary files and brute force lists and their hash values. It is a lookup table specially used in recovering a plaintext password from a cipher text. The attacker uses this table to look for the password and tries to recover it from password hashes.

Computed Hashes: An attacker computes the hash for a list of possible passwords and compares it to the pre-computed hash table (rainbow table). If attackers find a match, they can crack the password.

Compare the Hashes: An attacker captures the hash of a password and compares it with the precomputed hash table. If a match is found, then the password is cracked. It is easy to recover passwords by comparing captured password hashes to the pre-computed tables.



Tools to Create Rainbow Tables: rtgen and Winrtgen

Attackers can create rainbow tables by using the following tools.

- **rtgen**

  Source: *http://project-rainbowcrack.com*

  RainbowCrack is a general propose implementation that takes advantage of the time-memory trade-off technique to crack hashes. This project allows you to crack a hashed password. The rtgen tool of this project helps to generate the rainbow tables. The rtgen program needs several parameters to generate a rainbow table.

  The syntax of the command line is:

  Syntax: `rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index`

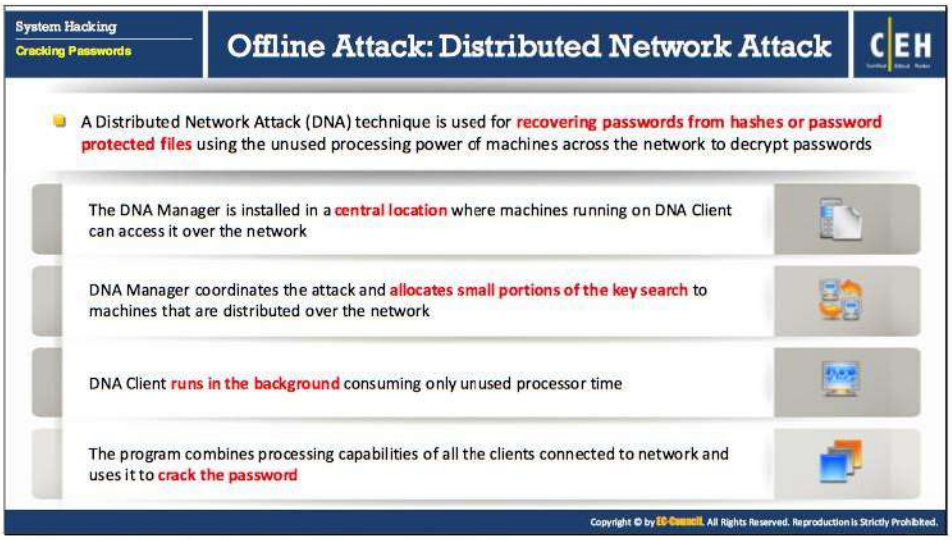
- **Winrtgen**

  Source: *http://www.oxid.it*

  Winrtgen is a graphical rainbow tables generator that helps attackers to create rainbow tables from which they can crack the hashed password. Winrtgen supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384), and SHA-2 (512) hashes.

  Generate rainbow tables using Winrtgen:

  1. Download and install **Winrtgen**. Click the **Add Table** button.
  2. In the **Rainbow Table properties** window, set up all of the properties, and click **OK**. In the main program, click **OK**.



Offline Attack: Distributed Network Attack

A Distributed Network Attack (DNA) is a technique used for recovering password-protected files that utilizes the unused processing power of machines across the network to decrypt passwords. In this attack, an attacker installs a DNA manager in a central location where machines running DNA clients can access it over a network. The DNA manager coordinates the attack, assigning small portions of the key search to machines distributed throughout the network. The DNA client runs in the background, only taking unused processor time. The program combines the processing capabilities of all the clients connected to the network and uses it to crack the password.

Features of the DNA:

- Reads statistics and graphs easily
- Adds user dictionaries to crack the password
- Optimizes password attacks for specific languages
- Modifies the user dictionaries
- Comprises the stealth client installation functionality
- Automatically updates client while updating the DNA server

On classification, the DNA splits into two modules:

- **DNA Server Interface**

  The DNA server interface allows users to manage DNA from a server. The DNA server module provides the user with the status of all jobs that the DNA server is executing. This interface contains:

- **Current jobs:** The current job queue consists of all jobs added to the list by the controller. The current job list has many columns, such as the identification number assigned by the DNA to the job, the name of the encrypted file, the user's password, the password that matches a key, which can unlock the data, the status of the job, and various other columns.
- **Finished jobs:** The finished job list provides information about the decryption jobs including the password. The finished job list also has many columns that are similar to the current job list. These columns include the identification number assigned by DNA to the job, the name of the encrypted file, the decrypted path of the file, the key used to encrypt and decrypt the file, the date and time that the DNA server started working on the job, the date and time the DNA server finished working on the job, the elapsed time, and so on.

- **DNA Client Interface**

  Users can use the DNA client interface from many workstations. The DNA client interface helps the client statistics to coordinate easily, and is available on machines with the pre-installed DNA client application. There are many components such as the name of the DNA client, the name of the group to which the DNA client belongs, the statistics about the current job, and many other components.

Network Management

The Network Traffic dialog box aids in the discovery of the network speed the DNA uses and each work-unit length of the DNA client. Using the work-unit length, a DNA client can work without contacting the DNA server. The DNA client application has the ability to contact the DNA server at the beginning and ending of the work-unit length.

The user can monitor the job status queue and the DNA. After collecting the data from Network Traffic dialog box, the user can modify the client work. When the size of the work-unit length increases, the speed of the network traffic decreases. Decrease in the speed of the traffic leads the client working on the jobs to spend longer amounts of time. Therefore, the user can make fewer requests to the server because of the reduction in bandwidth of network traffic.

Password Recovery Tools

Password Recovery tools allow attackers to break complex passwords, recover strong encryption keys, and unlock several documents.

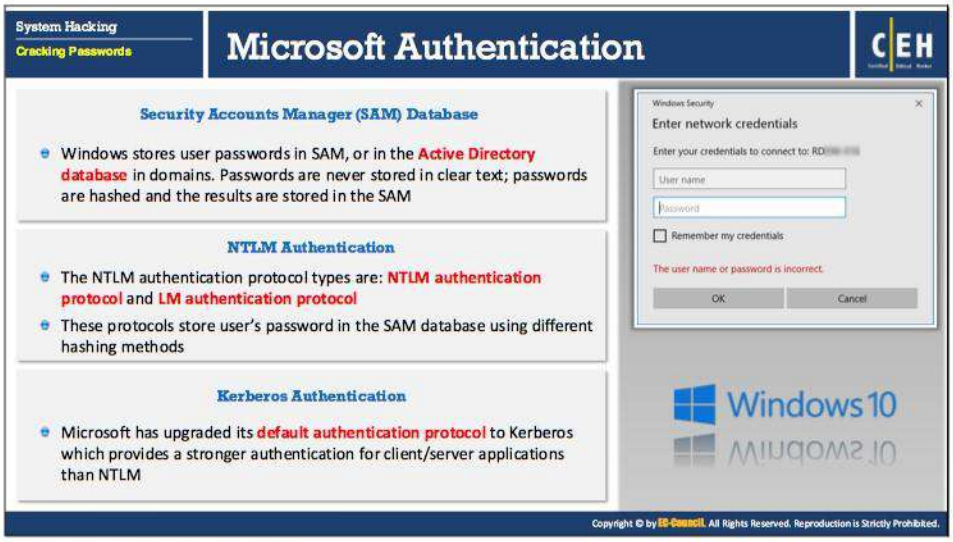
- **Elcomsoft Distributed Password Recovery**

  Source: *https://www.elcomsoft.com*

  The application allows attackers to break complex passwords, recover strong encryption keys, and unlock documents in a production environment. It allows for the execution of mathematically intensive password recovery code on the parallel computational elements found in modern graphic accelerators by employing an innovative technology to accelerate password recovery, when a compatible ATI or NVIDIA graphics card is present in addition to the CPU-only mode. When compared to password recovery methods that use only the computer's main CPU, the GPU acceleration used by this technology makes password recovery faster. This in turn supports password recovery using a variety of applications and file formats.

Some of the password recovery tools are listed below:

- Passware Kit Forensic (*https://www.passware.com*)
- WINDOWS PASSWORD RECOVERY TOOL ULTIMATE (*https://www.tenorshare.com*)
- Stellar Phoenix Password Recovery (*https://www.stellarinfo.com*)
- Windows Password Recovery Tool (*https://www.windowspasswordsrecovery.com*)
- PCUnlocker (*https://www.top-password.com*)
- iSumsoft Windows Password Refixer (*http://www.isumsoft.com*)
- hashcat (*https://hashcat.net*)



Microsoft Authentication

When users log in to a Windows computer, a series of steps is performed for user authentication. The Windows operating system authenticates its users with the help of three mechansims (protocols) provided by Microsoft.

- **Security Accounts Manager (SAM) Database**

  Windows uses the Security Accounts Manager (SAM) database or Active Directory Database to manage user accounts and passwords in the hashed format (one-way hash). The system does not store the passwords in plaintext format, but in hashed format, to protect them from attacks. The system implements SAM database as a registry file, and the Windows kernel obtains and keeps an exclusive file system lock on the SAM file. As this file consists of a file system lock, this provides some measure of security for the storage of passwords.

  It is not possible to copy the SAM file to another location in the case of online attacks. Because the system locks the SAM file with an exclusive file system lock, a user cannot copy or move it while Windows is running. The lock will not release until the system throws a blue screen exception or the operating system has shut down. However, to make the password hashes available for offline brute-force attacks, attackers can dump the on-disk contents of the SAM file using various techniques. The SAM file uses a SYSKEY function (in Windows NT 4.0 and later versions) to partially encrypt the password hashes.

  Even if hackers use subterfuge techniques to discover the contents, the encrypted keys with a one-way hash make it difficult to hack. In addition, some versions have a secondary key, making the encryption specific to that copy of the OS.

- **NTLM Authentication**

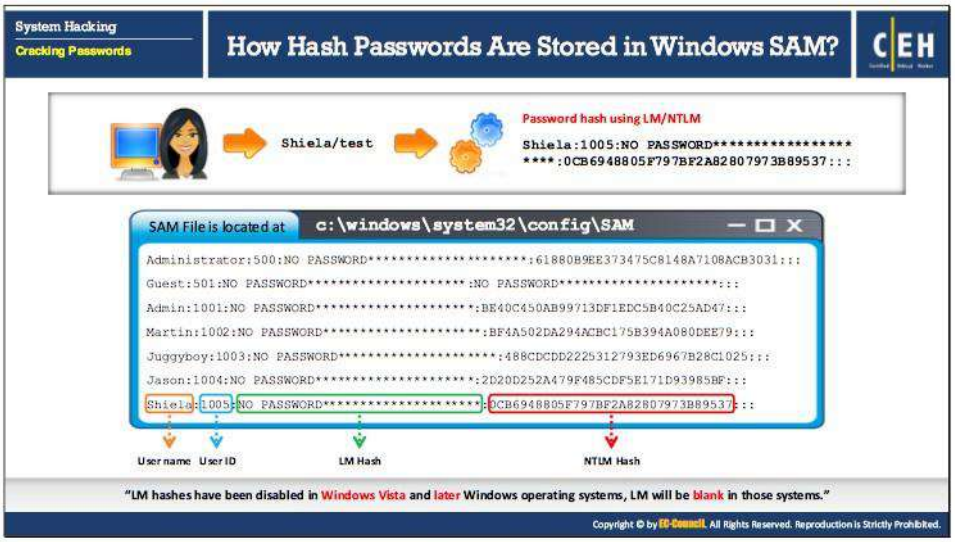
  NTLM (NT LAN Manager) is a default authentication scheme that performs authentication using a challenge/response strategy. Because it does not rely on any official protocol specification, there is no guarantee that it works correctly in every situation. It has been on some Windows installations, where it worked successfully. NTLM authentication consists of two protocols: NTLM authentication protocol and LM authentication protocol. These protocols use different hash methodology to store users' passwords in the SAM database.

- **Kerberos Authentication**

  Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography. This provides mutual authentication, in that both the server and the user verify each other's identity. Messages sent through Kerberos protocol are protected against replay attacks and eavesdropping.

  Kerberos makes use of the Key Distribution Center (KDC), a trusted third party. This consists of two logically distinct parts: an Authentication server (AS) and a Ticket Granting Server (TGS). Kerberos uses "tickets" to prove a user's identity.

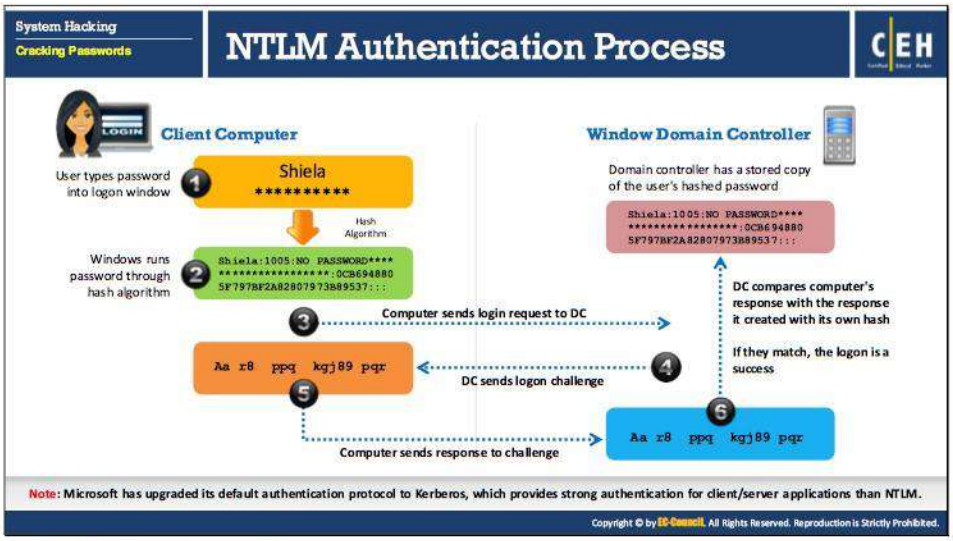
  Microsoft has upgraded its default authentication protocol to Kerberos which provides a stronger authentication for client/server applications than NTLM.



How Hash Passwords Are Stored in Windows SAM?

Windows operating systems use a Security Account Manager (SAM) database file to store user passwords. The SAM file is stored at %SystemRoot%/system32/config/SAM in Windows systems, and Windows mounts it in the registry, under the HKLM/SAM registry hive. It stores LAN Manager (LM) or NT LAN Manager (NTLM) hashed passwords.

NTLM supersedes the LM hash, which is susceptible to cracking. New versions of Windows still support LM hashes for backward compatibility; however, Vista and later Windows versions disable LM hash by default. The LM hash is blank in newer Windows versions. Selecting the option to remove LM hashes enables an additional check during password change operations but does not clear LM hash values from the SAM immediately: The SAM file stores a "dummy" value in its database, which bears no relationship to the user's actual password and is the same for all user accounts. It is not possible to calculate LM hashes for passwords exceeding 14 characters in length. Thus, the LM hash value is set to a "dummy" value when a user or administrator sets a password of more than 14 characters.



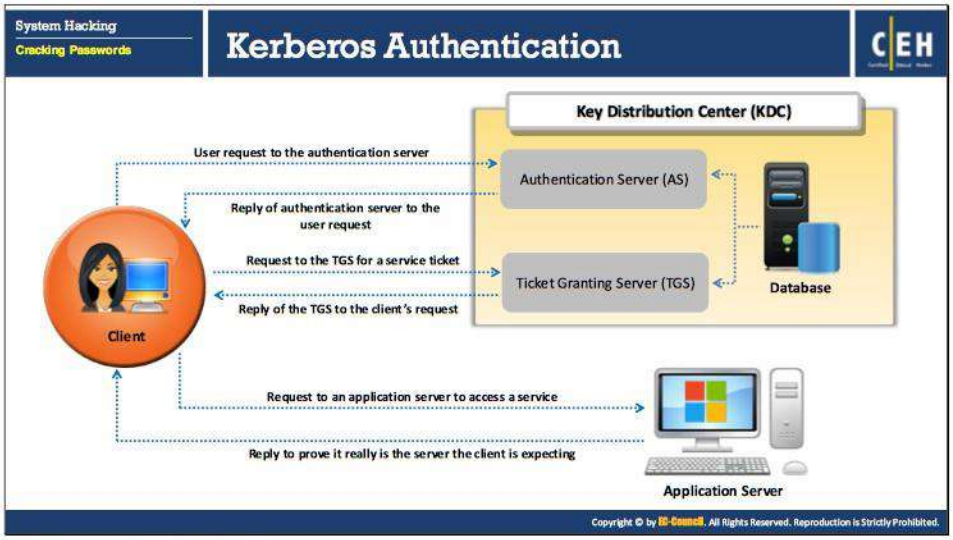
NTLM Authentication Process

NTLM includes three methods of challenge-response authentication: LM, NTLMv1, and NTLMv2, all of which use the same technique for the authentication process. The only difference among them is the level of encryption. In NTLM authentication, the client and server negotiate an authentication protocol. This is accomplished through the Microsoft negotiated Security Support Provider (SSP).

The following steps demonstrate the process and the flow of the client authentication to a domain controller using any NTLM protocol:

- The client types the user name and password into the logon window.
- Windows runs the password through a hash algorithm and generates a hash for the password that has been entered in the logon window.
- The client computer sends a login request along with domain name to the domain controller.
- The domain controller generates a 16-byte random character string called a "nonce" and sends it to the client computer.
- The client computer encrypts the nonce with a hash of the user password and sends it back to the domain controller.
- The domain controller retrieves the hash of the user password from the SAM and uses it to encrypt the nonce. The domain controller then compares the encrypted value with the value received from the client. A matching value authenticates the client and the logon is successful.

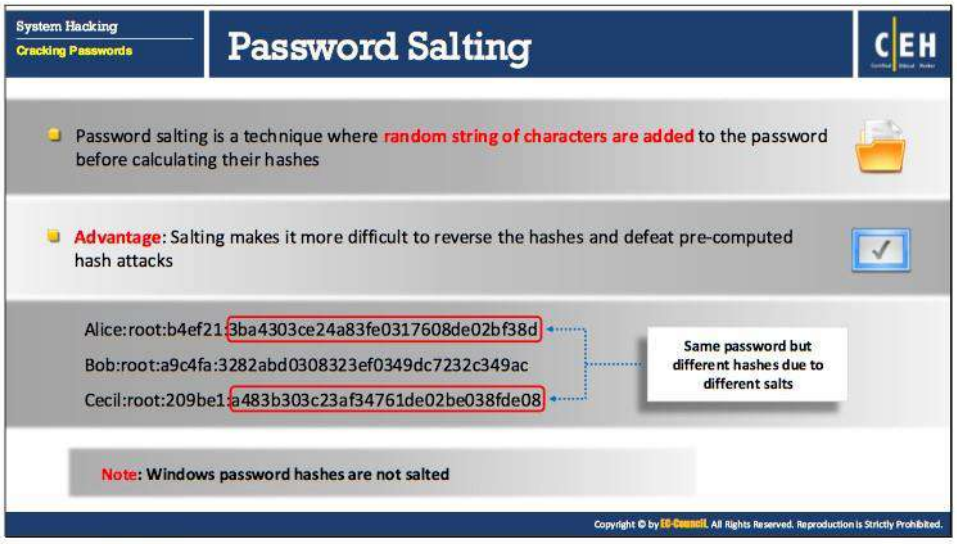
Note: Microsoft has upgraded its default authentication protocol to Kerberos, which provides a stronger authentication for client/server applications than NTLM.



Kerberos Authentication

Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography, which provides a mutual authentication. Both the server and the user verify each other's identity. Messages sent through the Kerberos protocol are protected against replay attacks and eavesdropping.

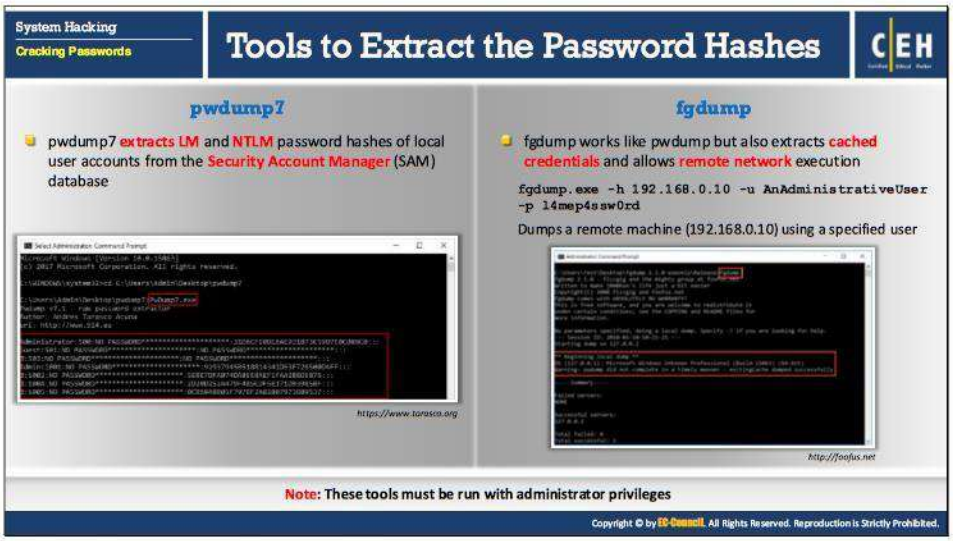
Kerberos makes use of the Key Distribution Center (KDC), a trusted third party, and consists of two logically distinct parts: an Authentication server (AS) and a Ticket Granting Server (TGS). The authorization mechanism of Kerberos provides the user with a Ticket Granting Ticket (TGT) that serves post-authentication for later access to specific services, Single Sign-On by which the user need not re-enter the password again for accessing any authorized services. It is important to note that there is no direct communication between the application servers and Key Distribution Center (KDC); the service tickets, even if packed by TGS, reach the service only through the client willing to access them.



Password Salting

Password salting is a technique where random strings of characters are added to the password before calculating their hashes. This makes it more difficult to reverse the hashes and defeats pre-computed hash attacks. The longer the random string, the harder it becomes to break or crack the password. The random string of characters should be a combination of alphanumeric characters.

In cryptography, a "salt" consists of random data bits used as an input to a one-way function, the other being a password. Instead of passwords, the output of the one-way function can be stored and used to authenticate users. A salt combines with a password by a key derivation function to generate a key for use with a cipher or other cryptographic algorithm. This technique generates different hashes for the same password. This makes cracking the passwords difficult.



Tools to Extract the Password Hashes

Use the following tools to extract the password hashes from the target system:

- **pwdump7**

  Source: *https://www.tarasco.org*

  pwdump7 is an application that dumps the password hashes (One Way Functions or OWFs) from NT's SAM database. pwdump extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database. This application or tool runs by extracting the binary SAM and SYSTEM File from the file system, and then extracts the hashes. One of the powerful features of pwdump7 is that it is also capable of dumping protected files. Pwdump7 is also able to extract passwords offline by selecting the target files. Use of this program requires administrative privileges on the remote system.

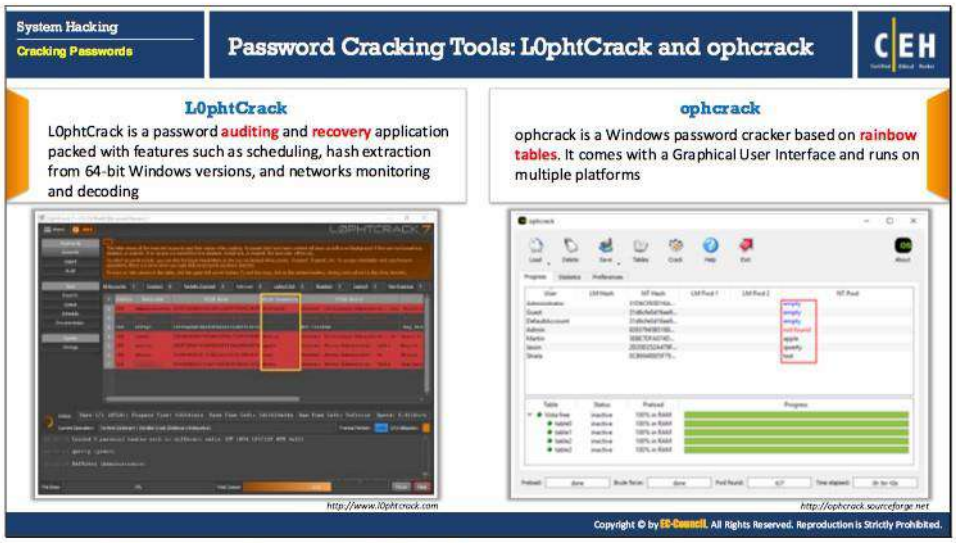
- **fgdump**

  Source: *http://foofus.net*

  Fgdump is a utility for dumping passwords on Windows NT/2000/XP/2003/Vista machines. It comes with built-in functionality that has all the capabilities of PWdump and can do a number of other crucial things such as execute a remote executable and dump the protected storage to a remote or local host, as well as grab cached credentials.

  Example:fgdump.exe -h 192.168.0.10 -u AnAdministrativeUser -p l4mep4ssw0rd

Note: Use of above tools requires administrative privileges on the remote system.



Password Cracking Tools: L0phtCrack and ophcrack

Password cracking tools allow you to reset unknown or lost Windows local administrator, domain administrator, and other user account passwords. In the case of forgotten passwords, it even allows users to get access to their locked computer instantly without reinstalling Windows. Attackers can use the password cracking tools to crack the passwords of the target system. Listed below are a few password cracking tools.

- **L0phtCrack**

  Source: *http://www.l0phtcrack.com*

  L0phtCrack is a tool designed to audit password and recover applications. It recovers lost Microsoft Windows passwords with the help of dictionary, hybrid, rainbow table, and brute-force attacks, and it also checks the strength of the password. LOphtCrack helps to disclose the security defects that are inherent in windows password authentication system.

  Some of its important features include scheduling, hash extraction from 64-bit Windows versions, multiprocessor algorithms, and networks monitoring and decoding.

  Features:

  - Operates on networks with Windows systems, including 32- and 64-bit environments, as well as most BSD and Linux variants with an SSH daemon
  - Performs scheduled scans depending on the organization's auditing requirements
  - Offers remediation assistance to system administrators on how to take action against accounts that have poor passwords on Windows systems

- Provides better user interface with more information about each user account, including password age, lock-out status, and whether the account is disabled, expired, or never expires
- Displays real-time reports in a separate, tabbed interface and displays auditing results based on the auditing method, risk severity, and password character sets
- Displays password risk status in four different categories: Empty, High Risk, Medium Risk, and Low Risk
- Reports the completion of the various password character sets being audited, including, Alpha, Alphanumeric, Alphanumeric/Symbol, Alphanumeric/Symbol/International
- Reports the overall length of the discovered password by account
- Delivers summary report of password statistics such as Locked, Disabled, Expired, or if the password is older than 180 days
- Delivers audit summary for the number of Accounts cracked and the number of Domains audited
- Cracks foreign passwords using foreign character sets for brute-force attacks, as well as foreign dictionary files

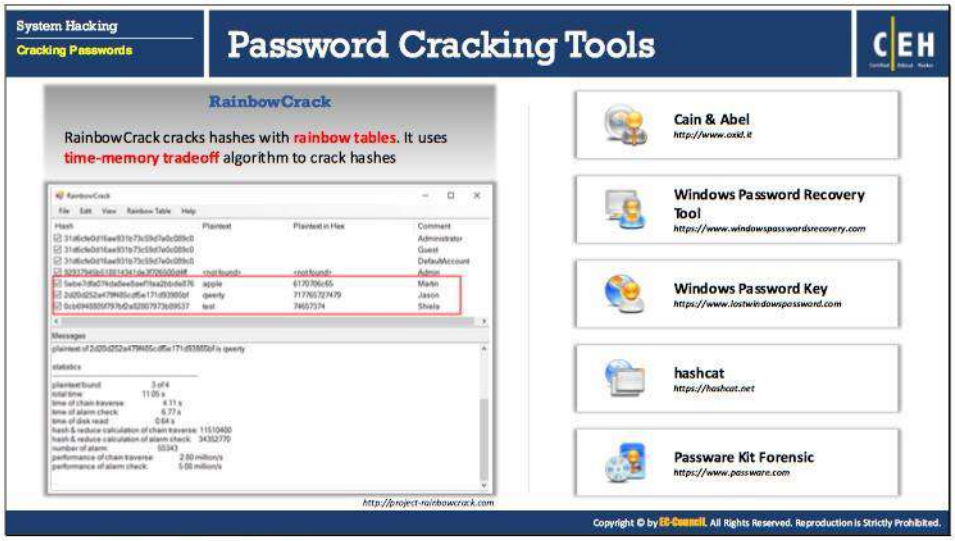
- **ophcrack**

  Source: *http://ophcrack.sourceforge.net*

  ophcrack is a Windows password cracking tool that uses rainbow tables for cracking passwords. It comes with a graphical user interface and runs on different operating systems such as Windows, Linux/Unix, etc.

  Features:

  - Cracks LM and NTLM hashes
  - Brute-force module for simple passwords
  - Real-time graphs to analyze the passwords
  - Dumps and loads hashes from encrypted SAM recovered from a Windows partition



Password Cracking Tools

- **RainbowCrack**

  Source: *http://project-rainbowcrack.com*

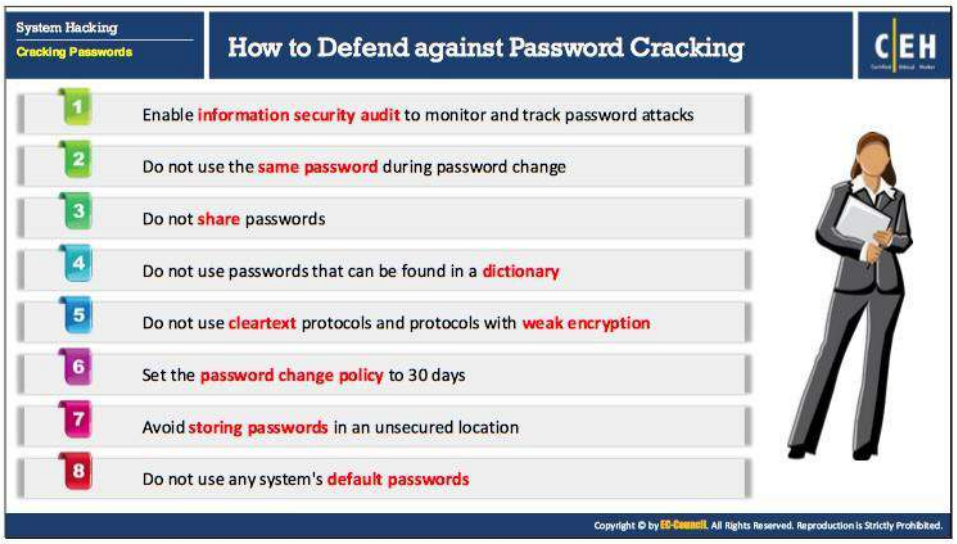
  RainbowCrack cracks hashes with rainbow tables, using a time-memory tradeoff algorithm. A traditional brute-force cracker cracks hashes differently than a time-memory-tradeoff hash cracker. The brute-force hash cracker will try all possible plaintexts one by one during cracking, whereas RainbowCrack pre-computes all possible plaintext hash pairs in the selected hash algorithm, charset, and plaintext length in advance and stores them in the "rainbow table" file. It may take a long time to pre-compute the tables, but once the pre-computation is finished, you will be able to crack the cipher text in the rainbow tables easily and quickly.

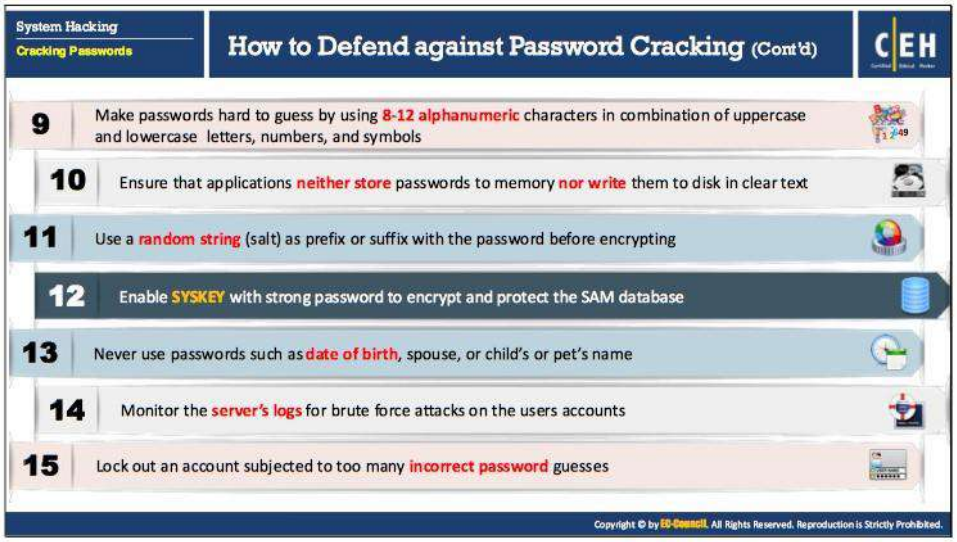
  Features:

  - Runs on Windows and Linux operating systems
  - Provides full time-memory tradeoff tool suites including rainbow table generation, sort, conversion, and lookup
  - Offers Unified rainbow table file format on all supported operating systems
  - Includes command-line user interface and Graphical user interface
  - Supports computation on multi-core processor
  - Supports rainbow table
    - For LM, NTLM, MD5 and SHA1 hash algorithms
    - In raw file format (.rt) and compact file format (.rtc) of any charset

Some of the password cracking tools are listed below:

- Cain & Abel (*http://www.oxid.it*)
- Windows Password Recovery Tool (*https://www.windowspasswordsrecovery.com*)
- Windows Password Key (*https://www.lostwindowspassword.com*)
- hashcat (*https://hashcat.net*)
- Passware Kit Forensic (*https://www.passware.com*)
- John the Ripper (*http://www.openwall.com*)
- THC-Hydra (*https://github.com*)
- InsidePro (*http://www.insidepro.com*)
- HashKiller.co.uk (*https://hashkiller.co.uk*)
- LSASecretsView (*http://www.nirsoft.net*)
- Password Cracker (*http://www.amlpages.com*)
- Windows Password Recovery (*https://www.passcape.com*)
- Password Recovery Bundle (*https://www.top-password.com*)
- JRecoverer Database Bundle(*http://www.lcpsoft.com*)
- Hash Suite (*http://hashsuite.openwall.net*)
- Medusa (*http://foofus.net*)
- Password Unlocker Bundle (*https://www.passwordunlocker.com*)
- Offline NT Password & Registry Editor (*https://pogostick.net*)
- Proactive System Password Recovery (*https://www.elcomsoft.com*)
- krbpwguess (*http://www.cqure.net*)





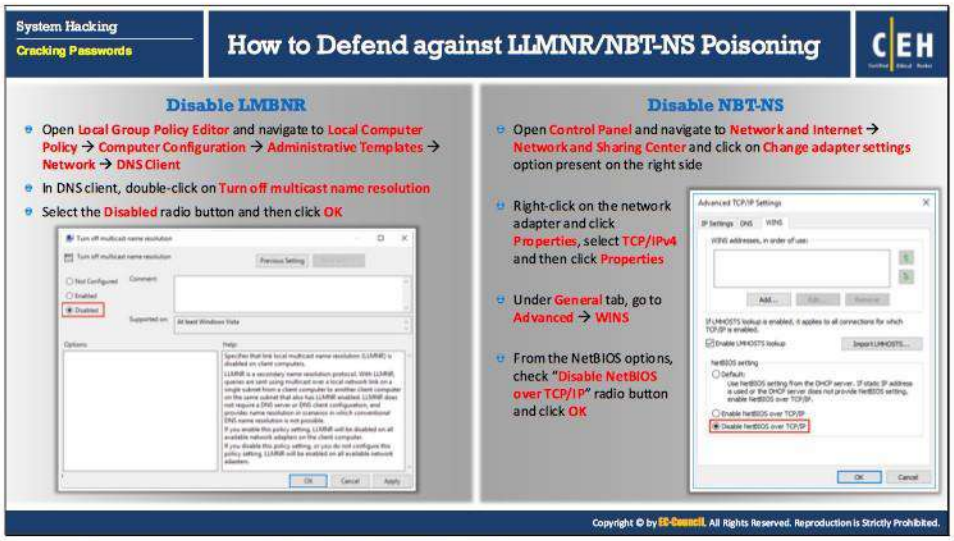
How to Defend against Password Cracking?

Best practices to protect against password cracking include:

- Enable information security audit to monitor and track password attacks
- Do not use the same password during password change
- Do not share passwords

- Do not use passwords that can be found in a dictionary
- Do not use cleartext protocols and protocols with weak encryption
- Set the password change policy to 30 days
- Avoid storing passwords in an unsecured location
- Do not use any system's default passwords
- Make passwords hard to guess by using 8 to 12 alphanumeric characters, using a combination of uppercase and lowercase letters, numbers, and symbols. Strong passwords are hard to guess. The more complex the password, the less it is subject to attacks.
- Ensure that applications neither store passwords to memory nor write them to disk in clear text. Passwords are always vulnerable to theft if they are stored in memory. Once the password becomes known, it is very easy for attackers to escalate their rights in the application.
- Use a random string (salt) as a password prefix or suffix before encrypting. It nullifies pre-computation and memorization. Because salt is usually different for each individual, it is impractical for attackers to construct tables with a single encrypted version of each candidate password. UNIX systems usually use a 12-bit set.
- Enable SYSKEY with a strong password to encrypt and protect the SAM database. Usually, the password information of user accounts is stored in the SAM database. It is very easy for password-cracking software to target the SAM database for accessing passwords. SYSKEY protects password information stored in the SAM data against password-cracking software through strong encryption techniques. It is more difficult to crack encrypted passwords than unencrypted ones.
- Never use personal information (e.g., birth date, or a spouse's, child's, or pet's name) to create passwords. Otherwise, it becomes quite easy for those close to you to crack those passwords.
- Monitor the server's logs for brute-force attacks on user accounts. Though brute-force attacks are difficult to stop, they are easily detectable by monitoring the web server log. For each unsuccessful login attempt, an HTTP 401 status code is recorded in the web server logs.
- Lock out an account that has been subjected to too many incorrect password guesses. This provides protection against brute-force and guessing attacks.
- Many password sniffers can be successful if LAN manager and NTLM authentication are used. Disable LAN manager and NTLM authentication protocols only after making sure that it does not affect the network.
- Perform a periodic audit of passwords in the organization.
- Check any suspicious application that stores passwords in memory or writes them to disk.

- Unpatched systems can reset passwords during buffer overflow or Denial of Service attacks. Make sure to update the system.
- Examine whether the account is in use, deleted or disabled. Disable the user account if multiple failed login attempts are detected.
- Enable account lockout with a certain number of attempts, counter time, and lockout duration.
- One of the most effective ways to manage passwords in organizations is to set an automated password reset.
- Make the system BIOS password-protected, particularly on devices that are susceptible to physical threats, such as servers and laptops.

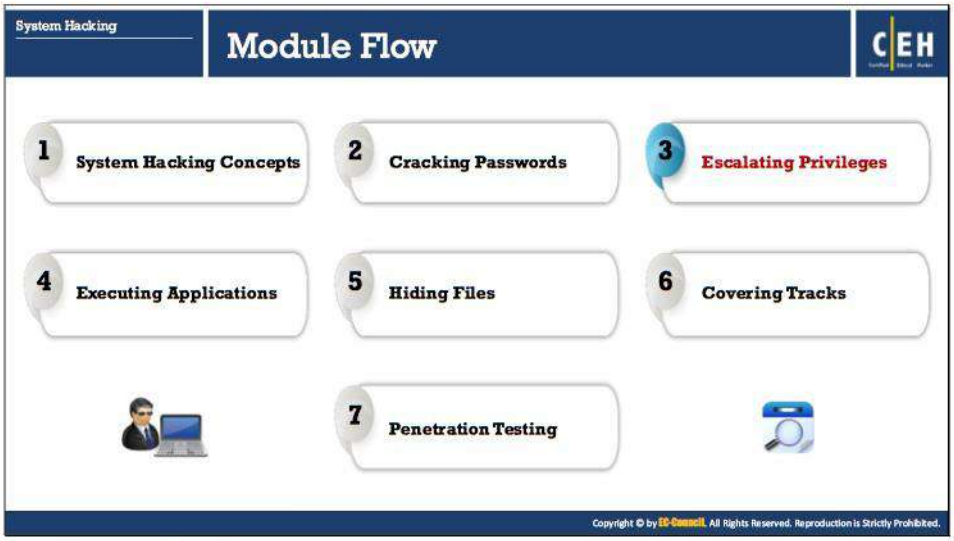


How to Defend against LLMNR/NBT-NS Poisoning

The easiest way to prevent a system from being attacked by a perpetrator is to disable both the LMNR and NBT-NS services in the Windows operating system. Attackers make use of these services in order to obtain user credentials and gain unauthorized access to the user's system.

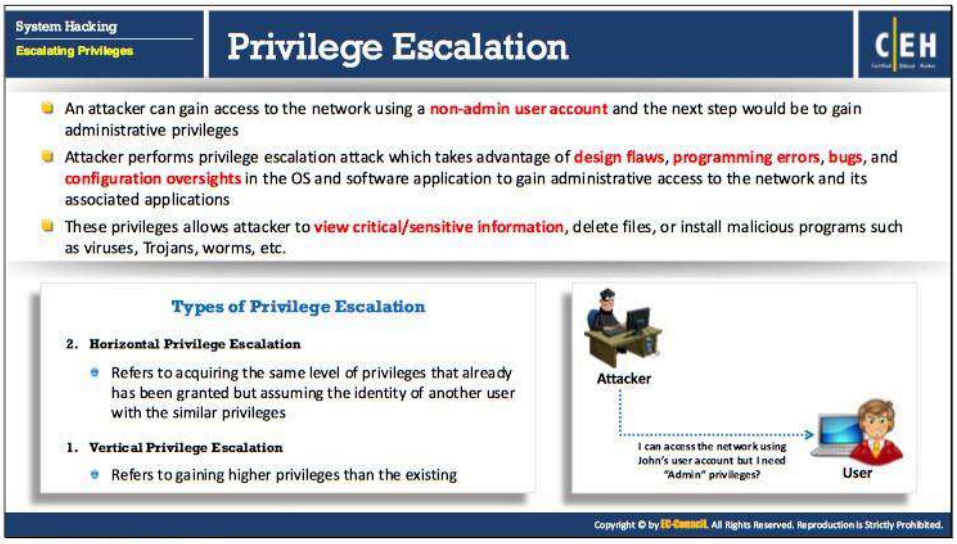
Steps to disable LLMNR/NBT-NS in any version of Windows:

- **Disabling LMBNR**
  - Open **Local Group Policy Editor**.
  - Navigate to **Local Computer Policy → Computer Configuration → Administrative Templates → Network →DNS Client**.
  - In DNS Client, double-click **Turn off multicast name resolution**.
  - Select the **Disabled** radio button and then click **OK**.
- **Disabling NBT-NS**
  - Open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center** and click on **Change adapter settings** option present on the right side.
  - Right-click on the network adapter and click **Properties**, select **TCP/IPv4** and then click **Properties**.
  - Under **General** tab, go to **Advanced → WINS**.
  - From the NetBIOS options, check **"Disable NetBIOS over TCP/IP"** radio button and click **OK**.



Escalating Privileges

Escalating privileges is the second stage of system hacking. Attackers use passwords obtained in the first step to gain access to the target system and then try to attain higher-level privileges in the system. The following topics explain various tool and techniques attackers use to escalate their privileges.



Privilege Escalation

Privileges are a security role assigned to users for using specific programs, features, operating systems, functions, files or codes, and so on, to limit their access by different types of users. If a user is assigned more privileges, he/she can modify or interact with a restricted part of the system or application than can less privileged users. Attackers first gain system access with less privilege, and then try to gain more privileges to perform activities restricted to less privileged users. Privilege escalation attack is the process of gaining more privileges than were initially acquired.

In a privilege escalation attack, attackers first gain access to the network using a non-admin user account, and then try to gain administrative privileges. Attackers take advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.

Once an attacker has gained access to a remote system with a valid username and password, he/she will attempt to escalate the user account to one with increased privileges, such as that of an administrator, to perform restricted operations. These privileges allow the attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

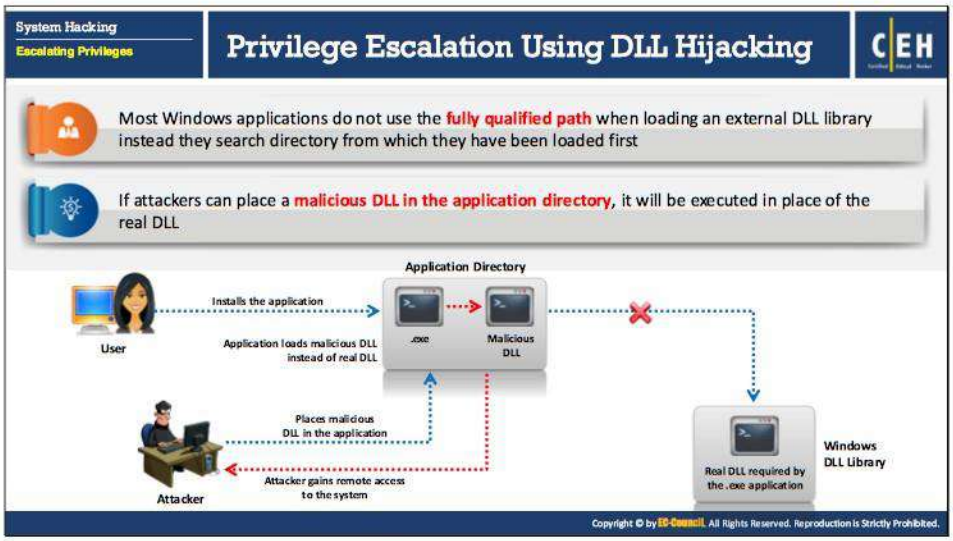
Types of Privilege Escalation

Privilege escalation is required when you want to access system resources that you are not authorized to access. Privilege escalation takes place in two forms. They are vertical privilege escalation and horizontal privilege escalation.

- **Horizontal Privilege Escalation:** In a horizontal privilege escalation, the unauthorized user tries to access the resources, functions, and other privileges that belong to the

authorized user who has similar access permissions. For instance, online banking user A can easily access user B's bank account.

- **Vertical Privilege Escalation:** In a vertical privilege escalation, the unauthorized user tries to gain access to the resources and functions of the user with higher privileges, such as application or site administrators. For example, someone performing online banking can access the site using administrative functions.



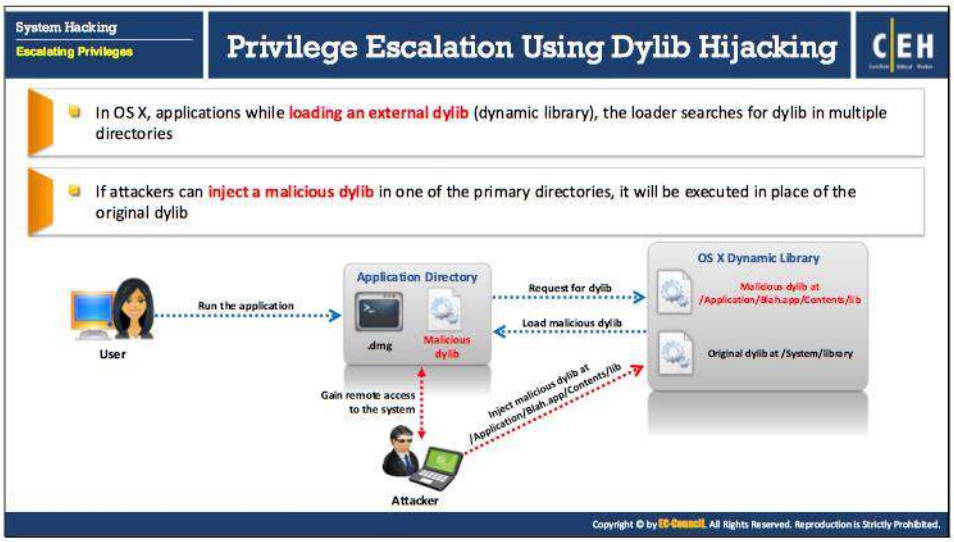
Privilege Escalation Using DLL Hijacking

Most Windows applications do not use the fully qualified path when loading an external DLL library; instead, they first search the directory from which they have been loaded. Taking this as an advantage, if attackers can place a malicious DLL in the application directory, the application will execute the malicious DLL in place of the real DLL. For example, if an application program ".exe" needs library.dll (usually in the Windows system directory) to install the application, and fails to specify the library.dll path, Windows will search for the DLL in the directory from which the application was launched. If an attacker has already placed the DLL in the same directory as program.exe, then that malicious DLL will load instead of the real DLL, which allows the attacker to gain remote access to the target system.

Privilege Escalation by Exploiting Vulnerabilities

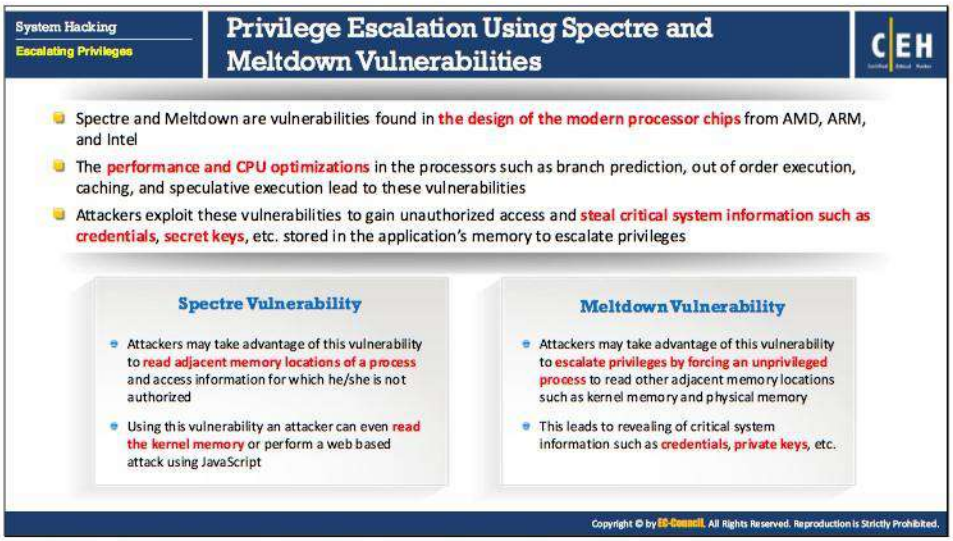
A vulnerability is an existence of a weakness, design, or implementation error that can lead to an unexpected event compromising the security of the system. An attacker takes advantage of these vulnerabilities to perform various attacks on confidentiality, availability, or integrity of a system. The software designing flaws and programming errors lead to security vulnerabilities. Attackers exploit these software vulnerabilities such as programming flaws in a program, service or within the operating system software or kernel to execute malicious code. Exploiting software vulnerabilities allows attackers to execute a command or binary on a target machine to gain higher privileges than the existing ones or bypass security mechanisms. Attackers using these exploits can even access privileged user accounts and credentials.

Many public vulnerability repositories are available online that allow access to information about various software vulnerabilities. Attackers search for an exploit based on the OS and software application on exploit sites such as SecurityFocus (http://www.securityfocus.com), Exploit Database (https://www.exploit-db.com)and use that exploit to gain higher privileges.



Privilege Escalation Using Dylib Hijacking

OS X similar to windows is vulnerable to dynamic library attacks. OS X provides several legitimate methods such as setting the DYLD_INSERT_LIBRARIES environment variable, which are user specific. These methods force the loader to load malicious libraries automatically into a target running process. OS X allows loading of weak dylibs (dynamic library) dynamically, which allows an attacker to place a malicious dylib in the specified location. In many cases, the loader searches for dynamic libraries in multiple paths. This helps an attacker to inject a malicious dylib in one of the primary directories and simply load the malicious dylib at runtime. Attackers can take advantage of such methods to perform various malicious activities such as stealthy persistence, run-time process injection, bypassing security software, bypassing Gatekeeper, etc.



Privilege Escalation using Spectre and Meltdown Vulnerabilities

Spectre and Meltdown are the recent CPU vulnerabilities found in the design of the modern processors including chips from AMD, ARM, and Intel. The performance optimizations in the modern processors led to these vulnerabilities. Attackers may take advantage of these vulnerabilities to gain unauthorized access and steal critical system information such as login credentials, secret keys, etc. stored in the application's memory to escalate privileges. These attacks can be performed because the normal verification of the user's privileges is disrupted through the interaction of features like branch prediction, out of order execution, caching, and speculative execution. Using these vulnerabilities attackers can exploit various IT resources such as most of the operating systems, servers, PCs, cloud systems, and mobile devices.

- **Spectre Vulnerability**

  Spectre vulnerability is found in many modern processors such as Apple, AMD, ARM, Intel, Samsung and Qualcomm processors. This vulnerability leads to tricking a processor to exploit speculative execution to read restricted data. The modern processors implement speculative execution to predict the future to complete the execution faster. For example, if the chip identifies that a program includes multiple conditional statements, it will start executing and concluding all the possible outputs before the program does. Attackers may exploit this vulnerability in different ways:

  - The processor is forced to accomplish a speculative execution of a read before bounds checking is performed. As a result, an attacker can access and read out of bound memory locations.
  - When executing conditional statements, for faster processing the processors use branch prediction to pick a path to speculatively execute. Attackers may exploit this

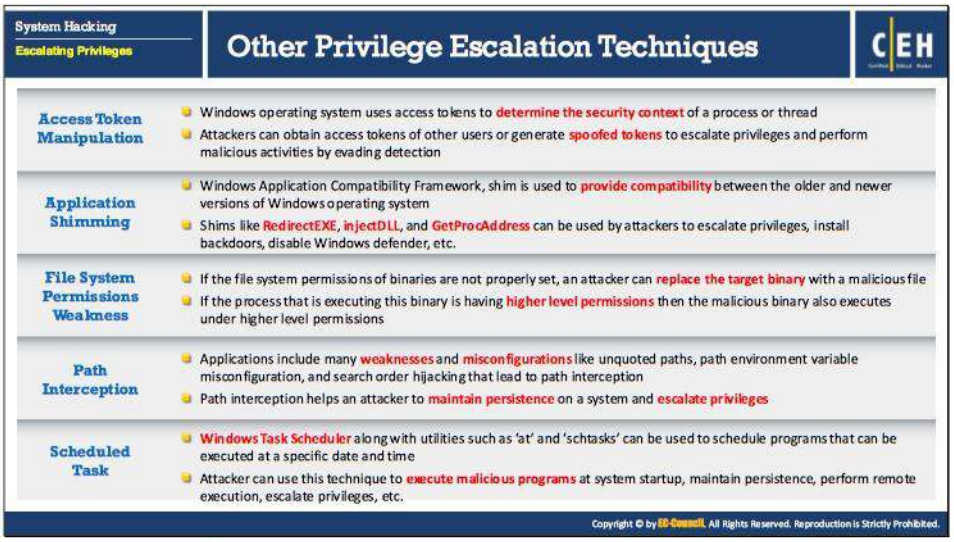
feature to force processor to take an improper speculative decision and further access data out of range.

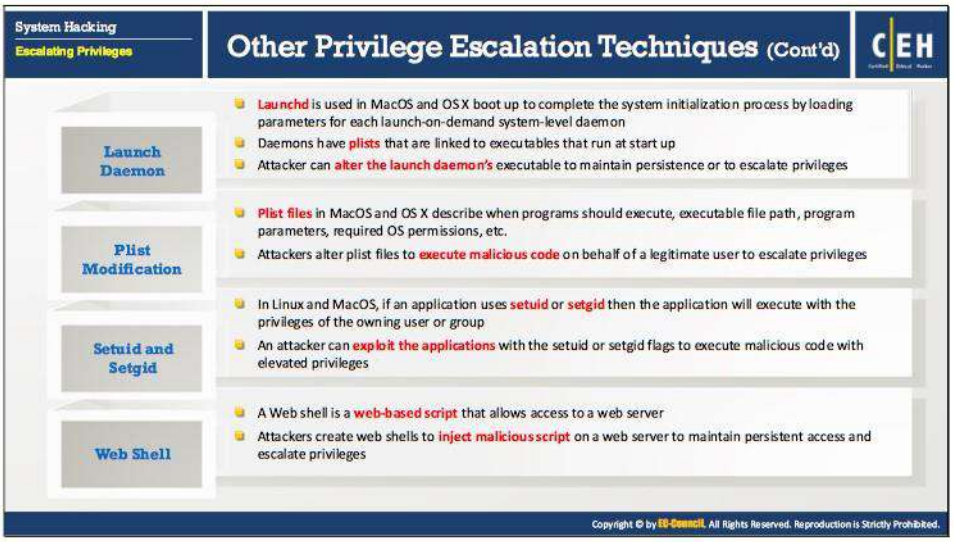
Attackers may use this vulnerability to read adjacent memory locations of a process and access information for which he/she is not authorized. This vulnerability helps attackers to extract confidential information such as credentials stored in the browser, from that target process. In certain cases, using this vulnerability an attacker can even read the kernel memory or perform a web based attack using JavaScript.

- **Meltdown Vulnerability**

  Meltdown vulnerability is found in all the Intel processors and ARM processors deployed by Apple. This vulnerability leads to tricking a process to access out of bounds memory by exploiting CPU optimization mechanisms such as speculative execution. For example, an attacker requests to access an illegal memory location. He/she sends a second request to conditionally read a valid memory location. In this case, the processor using speculative execution will complete evaluating the result for both requests before checking the first request. When the processor checks that the first request is invalid, it rejects both the requests after checking privileges. Even though the processor rejects both the requests, the result of both the requests remain in the cache memory. Now the attacker sends multiple valid requests to access out of bounds` memory locations.

  Attackers may use this vulnerability to escalate privileges by forcing an unprivileged process to read other adjacent memory locations such as kernel memory and physical memory. This leads to revealing of critical system information such as credentials, private keys, etc.





Other Privilege Escalation Techniques

- **Access Token Manipulation**

  In Windows operating system, access tokens are used to determine the security context of a process or thread. These tokens include the access profile (identity and privileges) of a user associated with a process. After a user is authenticated, the system produces an access token. Every process the user executes makes use of this access token. The system verifies this access token when a process is accessing a secured object.

Any Windows user can modify these access tokens so that the process seems to belong to some other user than the user who started this process. Then the process acquires the security context of the new token. For example, Windows Administrators have to log on as a normal user and need to run their tools with admin privileges using token manipulation command "runas". Attackers can take advantage of this to access tokens of other users or generate spoofed tokens to escalate privileges and perform malicious activities by evading detection.

- **Application Shimming**

  The Windows operating systems uses Windows Application Compatibility Framework called Shim to provide compatibility between the older and newer versions of Windows. For example, Application shimming allows programs created for Windows XP compatible with Windows 10. Shims provide buffer between the program and the operating system. This buffer is referenced when a program is executed to verify whether the program requires access to the shim database. When a program needs to communicate with the operating system, the shim database uses API hooking to redirect the code. All the shims installed by default Windows installer (sbinst.exe) are stored at

  `%WINDIR%\AppPatch\sysmain.sdb`

  `hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb`

  Shims run in user mode and they cannot modify the kernel. Some of these shims can be used to bypass UAC (RedirectEXE), inject malicious DLLs (InjectDLL), capture memory addresses (GetProcAddress) etc. An attacker can use these shims to perform different attacks such as disabling Windows defender, privilege escalation, installing backdoors, etc.

- **File System Permissions Weakness**

  Many processes in Windows operating system execute binaries automatically as part of their functionality or to perform certain actions. If the file system permissions of these binaries are not set properly then the target binary file may be replaced with a malicious file and it can be executed by the actual process. If the process that is executing this binary is having higher level permissions then the binary also executes under higher level permissions, which may include SYSTEM. Attackers can take advantage of this technique to replace original binaries with malicious binaries to escalate privileges. Attackers use this technique to manipulate Windows service binaries and self-extracting installers.

- **Path Interception**

  Path Interception is a method of placing an executable in a particular path in such a way that it will be executed by the application in place of the legitimate target. Attackers can take advantage of several flaws or misconfigurations to perform path interception like unquoted paths (service paths and shortcut paths), path environment variable

misconfiguration, and search order hijacking. Path interception helps an attacker to maintain persistence on a system and escalate privileges.

- **Scheduled Task**

  The Windows operating system includes utilities such as 'at' and 'schtasks'. A user with administrator privileges can use these utilities in conjunction with the Task Scheduler to schedule programs or scripts that can be executed at a particular date and time. If a user provides proper authentication, he can also schedule a task from a remote system using RPC. An attacker can use this technique to execute malicious programs at system startup, maintain persistence, perform remote execution, escalate privileges, etc.

- **Launch Daemon**

  At the time of MacOS and OS X booting process, launchd is executed to complete the system initialization process. Parameters for each launch-on-demand system-level daemon found in /System/Library/LaunchDaemonsand /Library/LaunchDaemons are loaded using launchd. These daemons have property list files (plist) that are linked to executables that run at the time of booting. Attackers can create and install a new launch daemon, which can be configured to execute at boot-up time using launchd or launchctlto load plist into concerned directories. The weak configurations allow an attacker to alter the existing launch daemon's executable to maintain persistence or to escalate privileges.

- **Plist Modification**

  In MacOS and OS X plist (property list) files include all the necessary information that is needed to configure applications and services. These files describe when programs should execute, executable file path, program parameters, essential OS permissions, etc. The plist files are stored at specific locations like /Library/Preferences (which execute with high-level privileges) and ~/Library/Preferences (which execute with user privileges). Attackers can access and alter these plist files to execute malicious code on behalf of a legitimate user and further use them as a persistence mechanism and escalate privileges.

- **Setuid and Setgid**

  In Linux and MacOS, if an application uses setuid or setgid then the application will execute with the privileges of the owning user or group respectively. Generally, the applications run under the current user's privileges. There are certain circumstances where the programs must be executed with elevated privileges but the user running the program does not need the elevated privileges. In this scenario, one can set the setuid or setgid flags for their applications. An attacker can exploit the applications with the setuid or setgid flags to execute malicious code with elevated privileges.

- **Web Shell**

  A Web shell is a web-based script that allows access to a web server. Web shells can be created in all the operating systems like Windows, Linux, MacOS and OS X. Attackers create web shells to inject malicious script on a web server to maintain persistent access

and escalate privileges. Attackers use a web shell as a backdoor to gain access and control a remote server. Generally, a web shell runs under current user's privileges. Using a web shell an attacker can perform privilege escalation by exploiting local system vulnerabilities. After escalating the privileges, an attacker can install malicious software, change user permissions, add or remove users, steal credentials, read emails, etc.

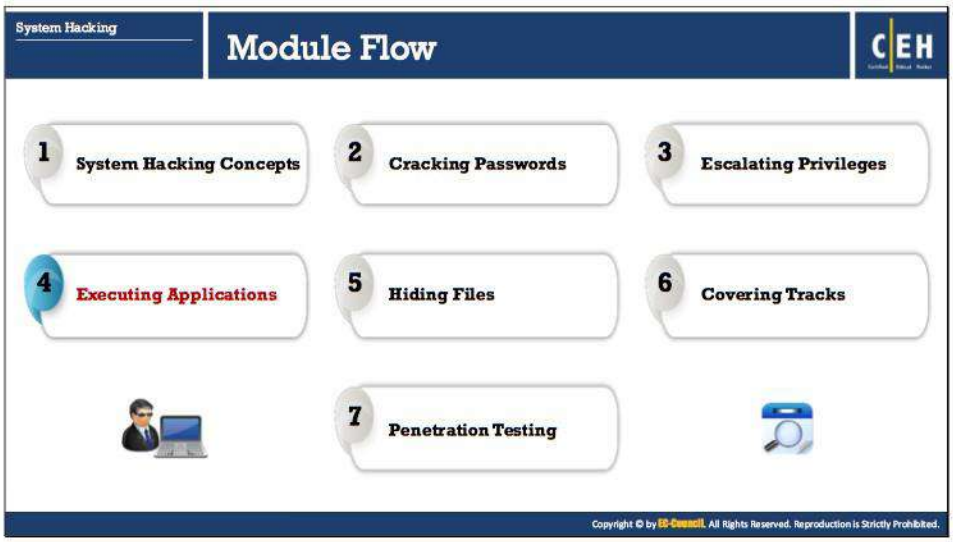
How to Defend Against Privilege Escalation

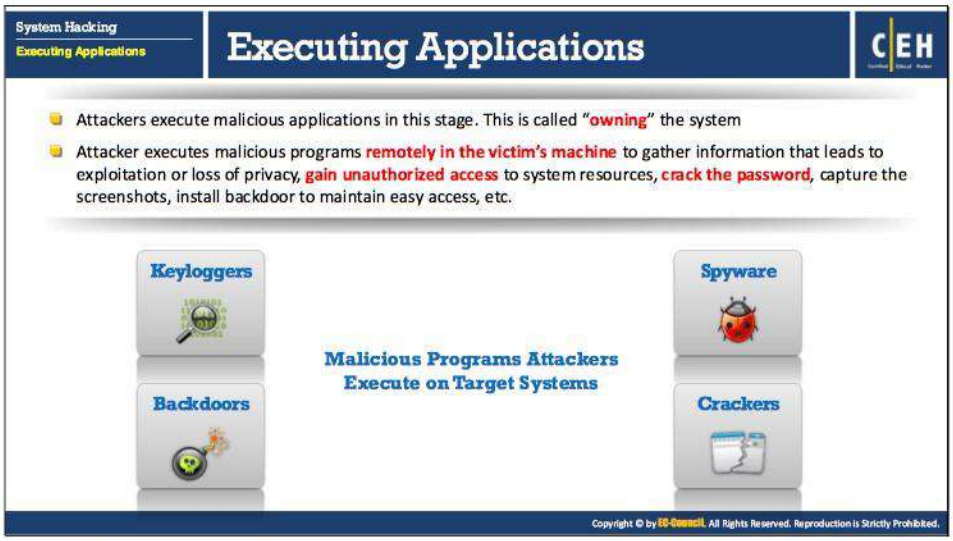
The best countermeasure against privilege escalation is to ensure that users have the least possible or just enough privileges to use their system effectively. In this case, even though the attacker succeeds in gaining access to the low privileged account, he/she will not be able to gain administrative level access. Often, flaws in programming code allow such escalation of privileges on a target system. As stated earlier, it is possible for an attacker to gain access to the

network using a non-administrative account, and then gain the higher privilege of an administrator.

The following are the best countermeasures to defend against privilege escalation:

- Restrict the interactive logon privileges
- Use encryption technique to protect sensitive data
- Run users and applications on the least privileges
- Reduce the amount of code that runs with particular privilege
- Implement multi-factor authentication and authorization
- Perform debugging using bounds checkers and stress tests
- Run services as unprivileged accounts
- Test operating system and application coding errors and bugs thoroughly
- Implement a privilege separation methodology to limit the scope of programming errors and bugs
- Patch and update the kernel regularly
- Change UAC settings to "Always Notify", so that it increases the visibility of the user when UAC elevation is requested
- Restrict users from writing files to the search paths for applications
- Continuously monitor file system permissions using auditing tools
- Reduce the privileges of user accounts and groups so that only legitimate administrators can make service changes
- Use whitelisting tools to identify and block malicious software that changes file, directory, and service permissions
- Use fully qualified paths in all the Windows applications
- Ensure that all executables are placed in write-protected directories
- In MAC operating systems, prevent plist files from being altered by users making them read-only
- Block unwanted system utilities or software that may be used to schedule tasks
- Patch and update the web servers regularly
- Disable the default local administrator account





Executing Applications

Once attackers gain higher privileges on the target system by trying various privilege escalation attempts, they may attempt to execute a malicious application by exploiting a vulnerability to execute arbitrary code. By executing malicious applications, the attacker can steal personal information, gain unauthorized access to system resources, crack passwords, capture screenshots, install a backdoor for maintaining easy access, and so on.

Attackers execute malicious applications in this stage in a process called "owning" the system. Once they acquire administrative privileges, they will execute applications. Attackers may even try to do so remotely on the victim's machine to gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources, crack passwords, capture screenshots, install a backdoor to maintain easy access, and so on.

The malicious programs attackers execute on target systems can be:

- **Backdoors**-Program designed to deny or disrupt operation, gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources.
- **Crackers**- Piece of software or program designed for cracking a code or passwords.
- **Keyloggers**- This can be hardware or a software type. In either case, the objective is to record each keystroke made on the computer keyboard.
- **Spyware**- Spy software may capture the screenshots and send them to a specified location defined by the hacker. To this purpose, attackers have to maintain access to victims' computers. After deriving all the requisite information from the victim's computer, the attacker installs several backdoors to maintain easy access to it in the future.

Tools for Executing Applications

Tools used for executing application remotely helps attackers perform various malicious activities on target systems. After gaining administrative privileges, attackers use these tools to install, execute, delete, and/or modify the restricted resources on the victim machine.

- **RemoteExec**

  Source: *https://www.isdecisions.com*

  RemoteExec remotely installs applications, executes programs/scripts, and updates files and folders on Windows systems throughout the network. It allows an attacker to modify the registry, change local admin passwords, disable local accounts, and copy/ update/delete files and folders.

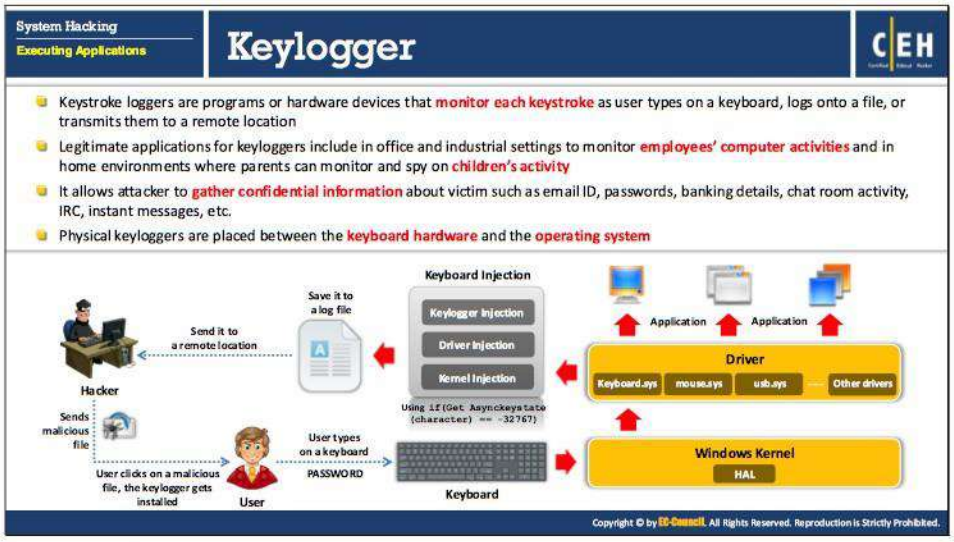
  RemoteExec can perform the following activities remotely.

  - **Remote MSI package Installation:** RemoteExec can remotely deploy applications developed using .msi format to a number of Windows systems by specifying the path of .msi file that the attacker wants to deploy, and then choosing the action (install/uninstall/repair/update) to perform.
  - **Remote Execution:** RemoteExec allows remote execution of programs (.exe, .bat, .cmd), scripts (.vbs, .js) and files associated to executables (.txt, .doc, .wav, .reg, .inf, .msi, etc.).
  - **Registry Modification:** RemoteExec allows the remote modification of the registry on all Windows systems throughout the network, or of a specific subset of computers. You just have to indicate the path to the .reg, select the target systems and launch with a click.

- **File Operations:** RemoteExec allows copying, updating, or deleting files and folders on Windows systems throughout the network.
- **Password and Local Account Management:** RemoteExec allows remotely changing the Local Administrator Password and disabling all other local accounts to reinforce security.
- **Interaction with Remote Systems:** RemoteExec enables you to remotely power off, reboot or shutdown systems, wake up computers equipped with Wake-On-LAN technology, and lock or close user sessions.

Some of the privilege escalation tools are listed below:

- PDQ Deploy (*https://www.pdq.com*)
- Dameware Remote Support (*https://www.dameware.com*)
- ManageEngine Desktop Central (*https://www.manageengine.com*)
- PsExec (*https://docs.microsoft.com*)
- TheFatRat (*https://github.com*)



Keylogger

Keyloggers are software programs or hardware devices that record the keys struck on the computer keyboard (also called keystroke logging) of an individual computer user or a network of computers. You can view all the keystrokes of the victim's computer at any time in your system by installing this hardware device or programs. It records almost all the keystrokes on a keyboard of a user and saves the recorded information in a text file. As Keyloggers hide their processes and interface, the target is unaware of the keylogging. Offices and industries use keyloggers for monitoring the employees' computer activities and in home environments in which parents can monitor children's Internet activities.

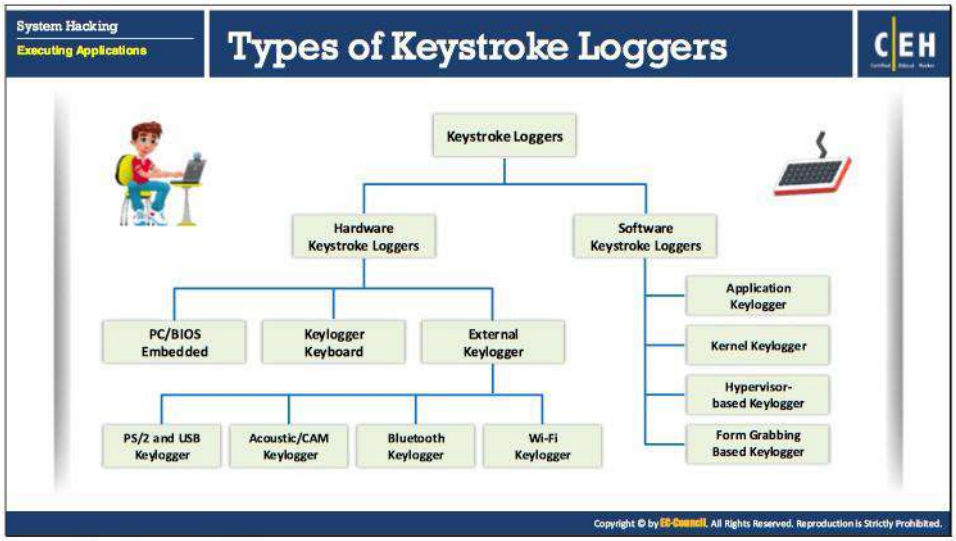
A keylogger, when associated with spyware, helps to transmit your information to an unknown third party. Attackers use it illegally for malicious purposes such as for stealing sensitive and confidential information about victims. The sensitive information includes email IDs, passwords, banking details, chat room activity, IRC, instant messages, and bank and credit card numbers. The data, transmitted over the encrypted Internet connection, are also vulnerable to keylogging, because the keylogger tracks the keystrokes before encryption.

The keylogger program is installed onto the user's system invisibly through email attachments or through "drive-by" downloads when users visit certain websites. Physical keystroke loggers "sit" between keyboard hardware and the operating system, so that they can remain undetected and record every keystroke.

A keylogger can:

- Record every keystroke typed on the user's keyboard
- Capture screenshots at regular intervals, showing user activity such as typed characters or clicked mouse buttons

- Track the activities of users by logging Window titles, names of launched applications, and other information
- Monitor online activity of users by recording addresses of the websites visited and with keywords entered
- Record all the login names, bank and credit card numbers, and passwords, including hidden passwords or data displayed in asterisks or blank spaces
- Record online chat conversations
- Make unauthorized copies of both outgoing and incoming email messages



Types of Keystroke Loggers

A keylogger is a hardware or software program that secretly records each keystroke on the user keyboard at any time. Keyloggers save captured keystrokes to a file for reading later or transmit them to a place where the attacker can access it. As these programs record all the keystrokes that are provided through a keyboard, they can capture passwords, credit card numbers, email address, names addresses, and phone numbers. Keyloggers have the ability to capture information *before* it is encrypted. This gives the attacker access to pass phrases and other "well-hidden" information.

There are two types of keystroke loggers: hardware key loggers and software key loggers. Both these keyloggers help attackers to record all keystrokes entered on the target system.

- **Hardware Keystroke Loggers**

  Hardware keyloggers are hardware devices look like normal USB drives. Attackers can connect these keyloggers between a keyboard plug and USB socket. All the keystrokes by the user are stored in the hardware unit. Attackers retrieve this hardware unit for accessing the keystrokes that are stored in it. The primary advantage of these loggers is that any antispyware, antivirus, or desktop security program cannot detect them. Its disadvantage is easy discovery of its physical presence.

  Hardware keystroke loggers are of three main types:

  - **PC/BIOS Embedded**

    BIOS-level firmware that is responsible for managing keyboard actions can be modified in such a way that it captures the keystrokes that are typed. It requires Physical and/or admin-level access to the target computer.

- **Keylogger Keyboard**

  By attaching the hardware circuit with the keyboard cable connector, it captures the key strokes. It records the all the keyboard strokes to its own internal memory that can be accessed later. The main advantage of a hardware key logger over a software key logger is that it is not operating system dependent and hence, it will not interfere with any applications running on the target computer, and it is impossible to discover hardware keyloggers by using any anti-keylogger software.

- **External Keylogger**

  External keyloggers are attached between a usual PC keyboard and a computer. They record each keystroke. External keyloggers do not need any software and work with any PC. You can attach them to your target computer and can monitor the recorded information on your PC to look through the keystrokes. There are four types of external keyloggers:

  - **PS/2 and USB Keylogger:** Completely transparent to computer operation and requires no software or drivers for the functionality. Record all the keystrokes typed by the user on the computer keyboard, and store data such as emails, chat records, applications used, IMs, and so on.
  - **Acoustic/CAM Keylogger:** Acoustic keyloggers work on the principle of converting electromagnetic sound waves into data. It makes use of either a capturing receiver capable of converting the electromagnetic sounds into the keystroke data or a CAM (camera) capable of recording screenshots of the keyboard.
  - **Bluetooth Keylogger:** Requires physical access to the target computer only once, at the time of installation. After installation on the target PC, it stores all the keystrokes and you can retrieve the keystroke information in real time by connecting via a Bluetooth device.
  - **Wi-Fi Keylogger:** Besides standard PS/2 and USB keylogger functionality, it features remote access over the Internet. This wireless keylogger will connect to a local Wi-Fi Access Point, and send E-mails containing recorded keystroke data. You can also connect to the keylogger at any time over TCP/IP and view the captured log.

- **Software Keystroke Loggers**

  These loggers are the software installed remotely via a network or email attachment in a target system for recording all the keystrokes. Here, the logged information is stored as a log file on a computer hard drive. The logger sends keystroke logs to the attacker using email protocols. Software loggers often have the ability to obtain additional data as well, because they do not have the limitation of physical memory allocations, as do hardware keystroke loggers.

  There are four types of software keystroke loggers:

- **Application Keylogger**

  An application keylogger allows you to observe everything the user types in his or her emails, chats, and other applications, including passwords. With this, you even can trace the records of Internet activity. It is an invisible keylogger to track and record everything happening within the entire network.

- **Kernel/Rootkit/Device Driver Keylogger**

  Attackers rarely use kernel keyloggers because it is difficult to write and requires a high level of proficiency from the keylogger developers. These keyloggers exist at the kernel level. Consequently, they are difficult to detect, especially for user-mode applications. This kind of keylogger acts as a keyboard device driver and thus gains access to all information typed on the keyboard.

  The rootkit-based keylogger is a forged Windows device driver that records all keystrokes. This keylogger hides from the system and is undetectable, even with standard or dedicated tools.

  This kind of keylogger usually acts as a device driver. The device driver keylogger replaces the existing I/O driver with the embedded keylogging functionality. This keylogger saves all the keystrokes performed on the computer into a hidden logon file, and then sends the file to the destination through the Internet.

- **Hypervisor-based Keylogger**

  A hypervisor-based keylogger works within a malware hypervisor operating on the operating system.

- **Form Grabbing Based Keylogger**

  Form-grabbing-based keylogger records the web form data and then submits it over the Internet, after bypassing https encryption. Form-grabbing-based keyloggers log web form inputs by recording web browsing on the Submit event function.

Hardware Keyloggers

Let us examine the details of external hardware keyloggers. As earlier discussed, there are various types of external hardware keyloggers available in the market. These keyloggers are plugged in-line, between a computer keyboard and a computer. These types of keyloggers include:

- PS/2 keylogger
- USB keylogger
- Wi-Fi keylogger
- Keylogger embedded inside the keyboard
- Bluetooth keylogger
- Hardware keylogger

These key loggers monitor and capture the keystrokes of the target system. As these external keyloggers attach between a usual PC keyboard and a computer to record each keystroke, these external hardware key loggers will remain undetectable by the anti-keyloggers installed on the target system. However, user can easily detect their physical presence.

There are various hardware keylogger manufacturers and vendors, some of which are discussed below.

- **KeyGrabber**

  Source: *https://www.keydemon.com*

  KeyGrabber hardware keylogger is an electronic device capable of capturing keystrokes from a PS/2 or USB keyboard. It provides various types of external hardware keyloggers such as KeyGrabber USB, KeyGrabber PS/2, and KeyGrabber Nano Wi-Fi.

Some of the hardware keyloggers are listed below:

- KeyCarbon (*http://www.keycarbon.com*)
- Keyllama Keylogger (*https://Keyllama.com*)
- Keyboard logger (*https://www.detective-store.com*)
- KeyGhost (*http://www.keyghost.com*)
- KeyCobra (*http://www.keycobra.com*)
- KEYKatcher (*https://keykatcher.com*)

Keyloggers for Windows

Besides the keyloggers explained previously, there are many software keyloggers available on the market; you can make use of these tools to record the keystrokes and monitor each activity of computer users. Some keyloggers are discussed below. You can download these tools from their respective web sites.

- **All In One Keylogger**

  Source: *http://www.relytec.com*

  All In One Keylogger is an invisible keylogger surveillance software that allows you to record keystrokes and monitors each activity of the computer user. It allows you to secretly track all such activities and automatically receive logs sent to the email/FTP/LAN account of your choice. The keylogger automatically activates itself when Windows starts and is completely invisible.

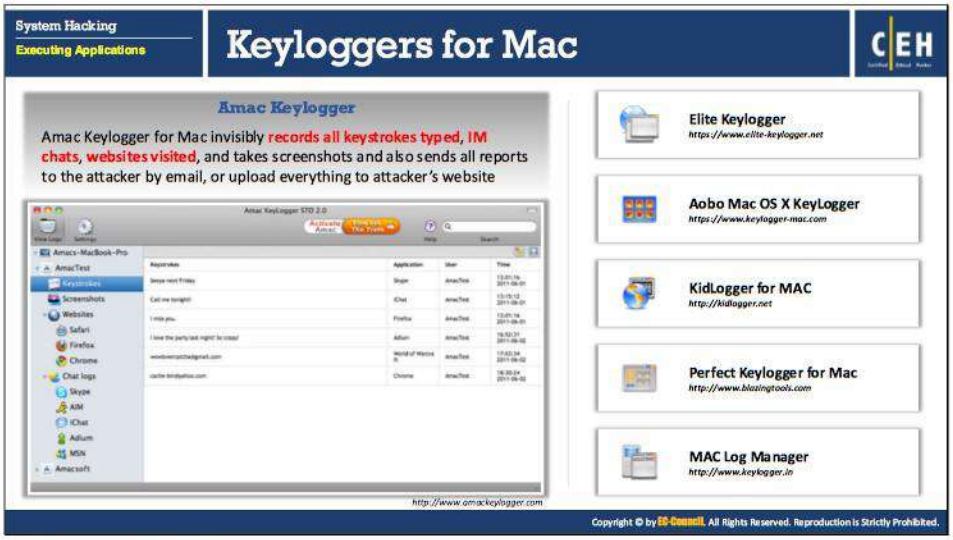
  You can perform the following actions using All In One Keylogger:

  - Capture all keystrokes (keystrokes logger)
  - Record instant messages
  - Monitor application usage
  - Capture desktop activity and take screenshots
  - Quick search over the log
  - Send reports via email, FTP, network
  - Record microphone sounds

- Generate and send HTML reports
- Disable anti keyloggers and unwanted software
- Filter monitored user accounts
- Block unwanted URLs
- Stop logging when the computer is idle

Some of the keyloggers for Windows are listed below:

- Spyrix Personal Monitor (*http://www.spyrix.com*)
- SoftActivity Activity Monitor (*https://www.softactivity.com*)
- Elite Keylogger (*https://www.elitekeyloggers.com*)
- Keylogger Spy Monitor (*http://ematrixsoft.com*)
- Micro Keylogger (*https://www.microkeylogger.com*)
- REFOG Personal Monitor (*https://www.refog.com*)
- Revealer Keylogger (*https://www.logixoft.com*)
- Realtime-Spy (*http://www.realtime-spy.com*)
- StaffCop Standard (*https://www.staffcop.com*)
- Ardamax Keylogger (*https://www.ardamax.com*)
- Ultimate Keylogger (*http://www.ultimatekeylogger.com*)
- Powered Keylogger (*http://www.mykeylogger.com*)
- Actual Keylogger (*http://www.actualkeylogger.com*)
- Spytector (*https://www.spytector.com*)
- Spy Keylogger (*http://www.spy-key-logger.com*)
- KidLogger (*https://kidlogger.net*)
- Advanced Keylogger (*http://www.mykeylogger.com*)
- KeyProwler (*https://keyprowler.com*)
- Keylogger (*https://github.com*)



Keyloggers for Mac

There are various keyloggers available on the market that run on the Mac operating system. These downloadable tools can assist an attacker in recording keystrokes and monitoring its users' activities. They enable you to record everything the user does on the computer, such keystroke logging, recording email communication, chat messaging, taking screenshots of each activity, and more.

The following keystroke loggers are specifically for use on the Mac OS:

- **Amac Keylogger**

  Source: *http://www.amackeylogger.com*

  Amac Keylogger for Mac OS X is a Mac application that allows users who want to spy on users of Macintosh computers and secretly record all information, including passwords, keystrokes, chat conversations, websites visited and screenshots captured. It also sends all reports to the attacker by email, or uploads everything to attacker's website.

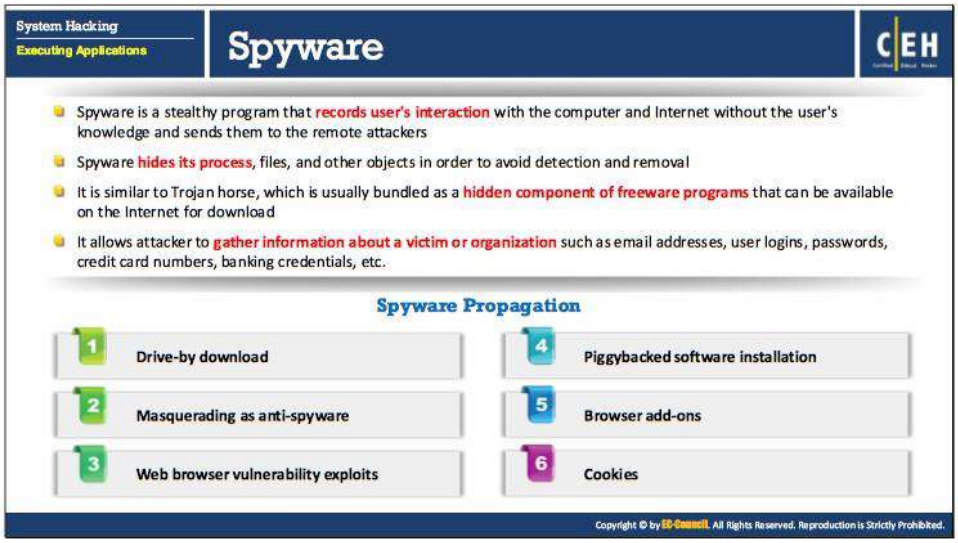
  Features:

  - Logs typed passwords
  - Logs keystrokes and chat conversations
  - Records websites and takes screenshots
  - Logs the Mac's IP address
  - Automatically runs at startup stealthily
  - Enables you to apply settings to all users with one click

- Sends logs to Email/FTP at preset intervals
- Password protects keylogger access

Some of the keyloggers for Mac are listed below:

- Elite Keylogger (*https://www.elite-keylogger.net*)
- Aobo Mac OS X KeyLogger (*https://www.keylogger-mac.com*)
- KidLogger for MAC (*http://kidlogger.net*)
- Perfect Keylogger for Mac (*http://www.blazingtools.com*)
- MAC Log Manager (*http://www.keylogger.in*)
- Award Keylogger for Mac (*http://www.award-soft.com*)
- Aobo Keylogger for Mac (*https://aobo.cc*)
- REFOG Keylogger for MAC (*https://www.refog.com*)
- FreeMacKeylogger (*http://www.hwsuite.com*)
- Spyrix Keylogger For Mac OS (*http://www.spyrix.com*)
- SniperSpy Mac (*http://www.sniperspymac.com*)
- Net Nanny for Mac (*https://www.netnanny.com*)
- Keyboard Spy Logger (*http://alphaomega.software.free.fr*)
- Keylogger (*https://github.com*)



Spyware

Spyware is stealthy computer monitoring software that allows you to secretly record all the user activities on the target computer. It automatically delivers logs to the remote attacker using Internet (via email, FTP, Command and Control through encrypted traffic, HTTP, DNS, etc.) The delivery logs include information about all areas of the system such as emails sent, websites visited, every keystroke (including login/password of Gmail, Facebook, Twitter, LinkedIn, etc.), file operations, and online chat conversations. It also takes screenshots at set intervals, just like a surveillance camera aimed at the computer monitor. Spyware is similar to a Trojan horse, which is usually bundled as a hidden component of freeware or software downloaded from the Internet. It hides its process, files, and other objects in order to avoid detection and removal. It allows an attacker to gather information about a victim or organization such as email addresses, user logins, passwords, credit card numbers, banking credentials, etc.

- **Spyware Propagation**

  As its name implies, the installation of spyware is done without user knowledge or consent, and can be accomplished by "piggybacking" the spyware onto other applications. This is possible because spyware uses advertising cookies, which is one of the spyware subclasses. Spyware can also affect your system when you visit a spyware distribution website. Because it installs itself when you visit and click something on a website; this process is known as "drive-by downloading."

  As a result of normal web surfing or downloading activities, the system may inadvertently become infected with spyware. It can even masquerade as antispyware and run on the user's computer without any notice, whenever the user downloads and installs programs that are bundled with spyware.

- **What Does the Spyware Do?**

  As discussed earlier, we are now familiar with spyware and its main function of keeping its eyes on user activities performed on the target computer. We also knew that once the attacker succeeds in installing spyware on a victim's computer anyway by means of propagation techniques discussed earlier, they can do many offensive things to the victim's computer. Now it is time to learn more about spyware capabilities other than simply monitoring users' activities.

  The installed spyware can also help the attacker perform the following on target computers:

  - Steals users' personal information and sends it to a remote server or hijacker
  - Monitors users' online activity
  - Displays annoying pop-ups
  - Redirects a web browser to advertising sites
  - Changes the browser's default setting and prevents the user from restoring
  - Adds several bookmarks to the browser's favorites list
  - Decreases overall system security level
  - Reduces system performance and causes software instability
  - Connects to remote pornography sites
  - Places desktop shortcuts to malicious spyware sites
  - Steals your passwords
  - Sends you targeted email
  - Changes the home page and prevents the user from restoring
  - Modifies the dynamically linked libraries (DLLs) and slows down the browser
  - Changes firewall settings
  - Monitors and reports websites you visit

- **Types of Spyware**

  Today, various spyware programs engage in a variety of offensive tasks, such as changing browser settings, displaying ads, collecting data, and so on. Though many spyware applications perform a diverse array of benign activities, 10 major types of spyware on the Internet allow attackers to steal information about users and their activities, all without their knowledge or consent.

  - **Desktop Spyware**

    Desktop spyware is software that allows an attacker to gain information about a user's activity or gather personal information about the user and send it via the

Internet to third parties without the user's knowledge or consent. It provides information regarding what network users did on their desktops, how, and when.

Desktop spyware allows attackers to perform the following:

- Live recording of remote desktops
- Recording and monitoring Internet activities
- Recording software usage and timings
- Recording activity log and storing at one centralized location
- Logging users' keystrokes

- **Email Spyware**

  Email spyware is a program that monitors, records, and forwards all incoming and outgoing email. Once installed on the computer that you want to monitor, this type of spyware records and sends copies of all incoming and outgoing emails to you through a specified email address or saves the information on the local disk folder of the monitored computer. This works in a stealth mode; users will not be aware of the presence of email spyware on their computer. It is also capable of recording instant messages (e.g., AIM, MSN, Yahoo, MySpace, Facebook).

- **Internet Spyware**

  Internet spyware is a utility that allows you to monitor all the web pages accessed by the users on your computer in your absence. It makes a chronological record of all visited URLs. This automatically loads at system startup and runs in stealth mode, which means that it runs in the background undetected. The utility records all visited URLs into a log file and sends it to a specified email address. It provides a summary report of overall web usage, such as websites visited, and the time spent on each website, as well as all applications opened along with the date/time of visits. It also allows you to block access to a specific web page or an entire website by specifying the URLs or keywords that you want blocked.

- **Child-Monitoring Spyware**

  Child-monitoring spyware allows you to track and monitor what children are doing on the computer, both online and offline. Instead of looking over the child's shoulder, one can use child monitoring spyware, which works in a stealth mode; your children will not be aware of your surveillance. The spyware logs all programs used, websites visited, counts keystrokes and mouse clicks, and captures screenshots of activity. All the recorded data is accessible through a password-protected web interface as a hidden, encrypted file or can be sent to a specified email address.

  This also allows you to protect children from accessing inappropriate web content by setting specific keywords that you want to block. It sends a real-time alert to you

whenever it encounters the specific keywords on your computer or whenever your children want to access inappropriate content.

- **Screen Capturing Spyware**

  Screen capturing spyware is a program that allows you to monitor computer activities by taking snapshots or screenshots of the computer on which the program is installed. This takes snapshots of the local or remote computer at specified time intervals and saves them either in a hidden file on the local disk or sends them to an email address or FTP site predefined by the attacker.

  Screen capturing spyware is not only capable of taking screenshots, but also captures keystrokes, mouse activity, visited website URLs, and printer activities in real time. The user can install this program or software led on networked computers to monitor the activities of all the computers on the network in real time by taking screenshots. This works transparently in stealth mode, so you can monitor computer activities without users' knowledge.

- **USB Spyware**

  USB spyware is a program designed for spying on the computer that copies spyware files from a USB device onto the hard disk without any request and notification. It runs in hidden mode, so users will not be aware of the spyware or the surveillance.

  USB spyware provides a multifaceted solution in the province of USB communications, as it is capable of monitoring USB devices' activity without creating additional filters, devices, and so on that might damage the system driver structure.

  USB spyware lets you capture, display, record, and analyze the data transferred between any USB device connected and a PC and its applications. This enables it to work on device drivers or hardware development, thus providing a powerful platform for effective coding, testing, and optimization, and makes it a great tool for debugging software.

  It captures all the communications between a USB device and its host and saves it into a hidden file for later review. A detailed log presents a summary of each data transaction, along with its support information. The USB spyware uses low system resources of the host computer. This works with its own timestamp to log all the activities in the communication sequence. USB spyware does not contain any adware or other spyware. It works with most recent variants of Windows.

  - USB spyware copies files from USB devices to your hard disk in hidden mode without any request
  - It creates a hidden file/directory with the current date and begins the background copying process
  - It allows you to capture, display, record, and analyze data transferred between any USB device connected to a PC and applications

- **Audio Spyware**

  Audio spyware is a sound surveillance program designed to record sound onto the computer. The attacker can install the spyware on the computer without the permission of the computer user in a silent manner without sending any notification to the user. The audio spyware runs in the background to record discreetly. Using audio spyware does not require any administrative privileges.

  Audio spyware monitors and records a variety of sounds on the computer, saving them in a hidden file on the local disk for later retrieval. Therefore, attackers or malicious users use this audio spyware to snoop and monitor conference recordings, phone calls, and radio broadcasts that might contain the confidential information.

  It is capable of recording and spying voice chat messages of various popular instant messengers. With this audio spyware, people can watch over their employees or children and see with whom they are communicating.

  It helps to monitor digital audio devices such as various messengers, microphones, and cell phones. It can record audio conversations by eavesdropping and monitor all ingoing and outgoing calls, text messages, and so on. They allow live call monitoring, audio surveillance, track SMS, logging all calls, and GPRS tracking.

- **Video Spyware**

  Video spyware is software for video surveillance installed on the target computer without the user's knowledge. All video activity can be recorded according to a programmed schedule. The video spyware runs transparently in the background, and secretly monitors and records webcams and video IM conversions. The remote access feature of video spyware allows the attacker to connect to the remote or target system to activate alerts and electric devices, and see recorded images in a video archive or even get live images from all the cameras connected to this system using a web browser such as Internet Explorer.

- **Print Spyware**

  Attackers can monitor the printer usage of the target organization remotely by using print spyware. Print spyware is printer usage monitoring software that monitors printers in the organization. Print spyware provides precise information about print activities for printers in the office or local printers, which helps in optimizing printing, saving costs, and so on. It records all information related to the printer activities, saves the information in encrypted log, and sends the log file to a specified email address over the Internet. The log report consists of the exact print job properties such as number of pages printed, number of copies, content printed, the date and time at which the print action took place.

  Print spyware records the log reports in different formats for various purposes such as a web format for sending the reports to an email through the web or the Internet and in hidden encrypted format to store on the local disk. The log reports generated will help attackers in analyzing printer activities. The log report shows how many

documents each employee or workstation printed, along with the time period. This helps in monitoring printer usage and to determine how employees are using the printer. This software also allows limiting access to the printer. This log report helps attackers to trace out information about sensitive and secret documents printed.

- **Telephone/ Cellphone Spyware**

  Telephone/cell phone spyware is a software tool that gives you full access to monitor a victim's phone or cell. It will completely hide itself from the user of the phone. It will record and log all activity on the phone such as Internet use, text messages, and phone calls. Then you can access the logged information via the software's main website, or you can also get this tracking information through SMS or email. Usually, this spyware helps to monitor and track phone usage of employees. But attackers are using this spyware to trace information from their target person's or organization's telephones/cell phones. Using this spyware doesn't require any authorized privileges.

  Most common telephone/cellphone spyware features include:

  - **Call History:** Allows you to see the entire call history of the phone (both incoming and outgoing calls).
  - **View Text Messages:** Enables you to view all incoming and outgoing text messages. It even shows deleted messages in the log report.
  - **Web Site History:** Records the entire history of all websites visited through the phone in the log report file.
  - GPS Tracking: Shows you where the phone is in real time. There is also a log of the cell phone's location so you can see where the phone has been.

    It works as depicted in the following diagram.

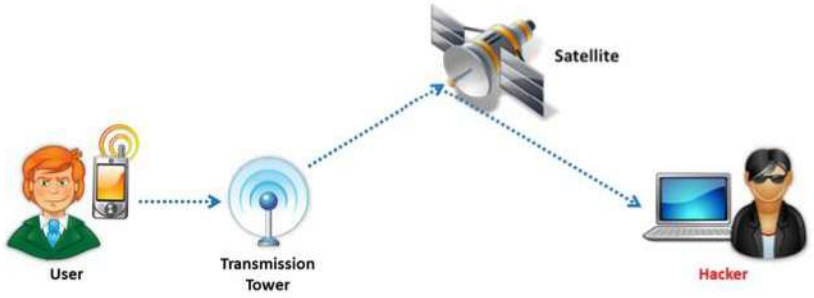


FIGURE 6.1: Telephone/cellphone spyware

- **GPS Spyware**

  GPS spyware is a device or software application that uses the Global Positioning System (GPS) to determine the location of a vehicle, person, or other attached or installed asset. An attacker can use this software to track the target person.

This spyware allows you to track the phone location points and saves or stores them in a log file and sends them to the specified email address. You can then watch the target user location points by logging into the specified email address, and it displays the connected point's trace of the phone location history on a map. It also sends email notifications of location proximity alerts. An attacker traces the location of the target person using GPS spyware, as shown in the following figure.

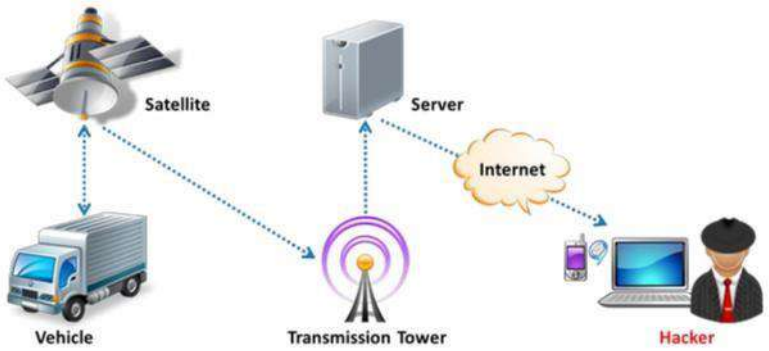


FIGURE 6.2: GPS spyware

Spyware Tools

- **Spytech SpyAgent**

  Source: *https://www.spytech-web.com*

  Spytech SpyAgent is a computer spy software that allows you to monitor everything users do on your computer—in total secrecy. SpyAgent provides a large array of essential computer monitoring features, as well as website, application, and chat client blocking, logging scheduling, and remote delivery of logs via email or FTP.

  It can also allow you to monitor following things on a user's computer:

  - It can reveal all websites visited
  - It records all online searches performed
  - It monitors what programs and apps are in use
  - It can track all file usage and printing information
  - It records online chat conversations
  - It is also able to see every email communication on the user's computer
  - It helps you determine what the user is uploading and downloading
  - It uncovers secret user passwords
  - It monitors social networking behaviors

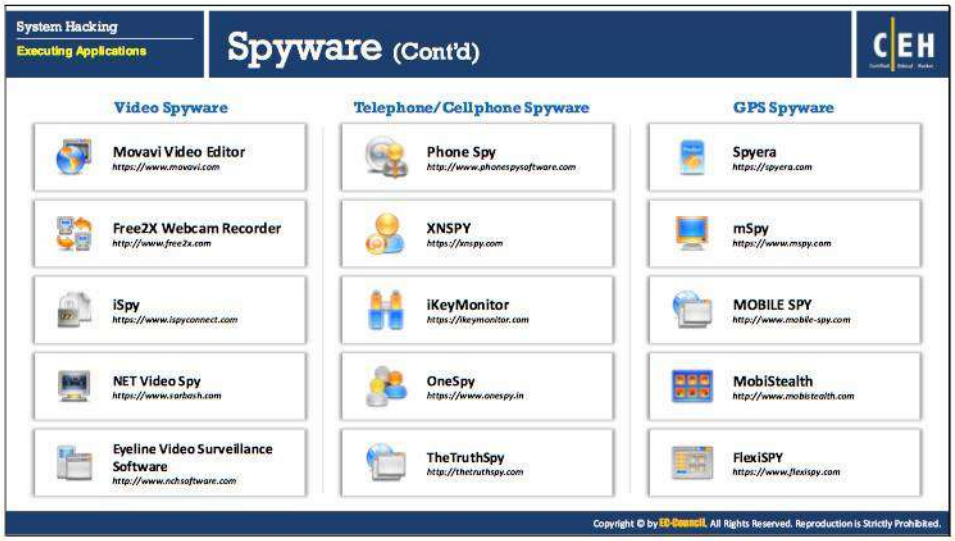
- **Power Spy**

  Source: *http://ematrixsoft.com*

  Power Spy is a PC-user activity monitoring software. It runs and performs monitoring secretly in the background of computer system. It logs all users on the system and users will not know its existence. After you install the software on the PC you want to monitor, you can receive log reports via emails or FTP from a remote location, for example, every hour. Therefore, you can read these reports anywhere, on any device at any time as long as you have Internet access. Power Spy lets you know exactly what others do on the PC while you are away.

  Features:

  - **Screen Recording:** Power Spy Software automatically captures screenshots of an entire desktop or active windows at set intervals, saves screenshots as JPEG format images on your hard disk, or sends them to you with text logs and automatically stops screenshot when monitored users are inactive.
  - **Keylogger:** The software logs all keystrokes, including optional non-alphanumeric keys, with a time stamp, Windows username, and application name and window caption. This includes all user names and passwords typed with program window caption.
  - **Instant Message and Chat Recording:** It monitors and records IM and chats in Skype, Yahoo Messenger, ICQ, and AIM. It includes both incoming and outgoing information with time stamps and user IDs.
  - **Email Recording:** Power Spy records all emails read in Microsoft Outlook, Microsoft Outlook Express, Win Mail, Windows Live Mail.
  - **Website URL Recording:** Monitors and records all URLs visited with Windows username and timestamp. It logs all webpages opened in Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Netscape, Avant Browser, Maxthon, NetCaptor, and any other web browsers.
  - **Application Recording:** It logs all applications executed, including the location of executable file, documents and directories navigated with time, Windows username, by application/document/directory name and file path.
  - **Document Recording:** Power Spy logs all text contents of documents opened in Microsoft Word, Windows WordPad and Windows Notepad. The software will record the same document only once in a log report to reduce its size.
  - **Clipboard Text Recording:** The software offers clipboard monitoring feature.



Spyware

The following is the list of spyware:

- **Desktop and Child Monitoring Spyware**
  - ACTIVTrak (*https://activtrak.com*)
  - Veriato 360 (*http://www.veriato.com*)

- NetVizor (*https://www.netvizor.net*)
- Activity Monitor (*https://www.softactivity.com*)
- SoftActivity TS Monitor (*https://www.softactivity.com*)
- Veriato Investigator (*http://www.veriato.com*)
- Personal Inspector (*http://www.spyarsenal.com*)
- Spytech SentryPC (*https://www.spytech-web.com*)
- Screenshot Monitor (*https://screenshotmonitor.com*)
- Teramind (*https://www.teramind.co*)
- EKRAN Employee Monitoring Software (*https://www.ekransystem.com*)
- REFOG Employee Monitor (*https://www.refog.com*)
- Net Nanny Home Suite (*https://www.netnanny.com*)
- Employee Desktop Live Viewer (*https://www.nucleustechnologies.com*)
- OsMonitor (*http://www.os-monitor.com*)
- Hubstaff Employee Monitoring Software (*https://hubstaff.com*)
- iMonitor EAM (*https://www.imonitorsoft.com*)
- iProtectYou Pro (*https://www.softforyou.com*)
- Child Control 2017 (*https://www.salfeld.com*)
- InterGuard (*https://www.interguardsoftware.com*)
- Aobo Filter for PC (*http://www.aobo-porn-filter.com*)

- **USB Spyware**

  USB spyware monitors and analyzes data transferred between any USB device connected to a computer and its applications. It helps in application development, USB device driver or hardware development and offers a powerful platform for effective coding, testing, and optimization.

  The following is the list of USB spyware:

  - USB Analyzer (*https://www.eltima.com*)
  - USB Monitor (*https://www.hhdsoftware.com*)
  - USBDeview (*http://www.nirsoft.net*)
  - Advanced USB Port Monitor (*https://www.aggsoft.com*)
  - USB Monitor Pro (*http://www.usb-monitor.com*)
  - Free USB Analyzer (*https://freeusbanalyzer.com*)
  - USBlyzer (*http://www.usblyzer.com*)

- Usb Sniffer for Windows (*https://sourceforge.net*)
- USBTrace (*http://www.sysnucleus.com*)
- KeyCarbon USB (*http://www.keycarbon.com*)
- USB 2GB Keylogger WiFi (*http://diij.com*)

- **Audio Spyware**

  Audio spyware helps to monitor sound and voice recorders on the system. It invisibly starts recording once it detects sound and automatically stops recording when the voice disappears. It can be used in recording conferences, monitoring phone calls, radio broadcasting logs, spying and employee monitoring, etc.

  The following is the list of USB spyware:

  - Spy Voice Recorder (*http://www.mysuperspy.com*)
  - Spy Audio Listening Device (*http://www.securityplanet.co*)
  - Spy USB Voice Recorder (*http://www.securityplanet.co*)
  - Audio Spy (*http://www.topsecretsoftware.com*)
  - Voice Activated Flash Drive Voice Recorder (*http://www.spytecinc.com*)

- **Video Spyware**

  Video Spyware is used for secret video surveillance. An attacker can use this software to secretly monitor and record webcams and video IM conversions. An attacker can use video spyware to remotely view webcams in order to get live footage of secret communication. With the help of this spyware, attackers can record and play anything displayed on victim's screen.

  The following is the list of Video spyware:

  - Movavi Video Editor (*https://www.movavi.com*)
  - Free2X Webcam Recorder (*http://www.free2x.com*)
  - iSpy (*https://www.ispyconnect.com*)
  - NET Video Spy (*https://www.sarbash.com*)
  - Eyeline Video Surveillance Software (*http://www.nchsoftware.com*)
  - WebcamMagic (*http://www.robomagic.com*)
  - WebCam Looker (*http://felenasoft.com*)
  - SecuritySpy (*http://www.bensoftware.com*)
  - 1AVMonitor (*http://www.pcwinsoft.com*)
  - Digi-Watcher (*http://www.digi-watcher.com*)
  - VRS Recording System (*http://www.nch.com.au*)

- CapturixVideoSpy (*http://www.capturix.com*)

- **Cellphone Spyware**

  Like Mobile Spy, an attacker can also use the following software programs as telephone/cell phone spyware to record all activity on a phone such as Internet usage, text messages and phone calls, and so on.

  The following are some available telephone/cell phone spyware programs:

  - Phone Spy (*http://www.phonespysoftware.com*)
  - XNSPY (*https://xnspy.com*)
  - iKeyMonitor (*https://ikeymonitor.com*)
  - OneSpy (*https://www.onespy.in*)
  - TheTruthSpy (*http://thetruthspy.com*)
  - MobileSpyAgent (*http://www.mobilespyagent.com*)
  - PhoneSheriff (*http://www.phonesheriff.com*)
  - FlexiSPY (*https://www.flexispy.com*)
  - MobiStealth (*http://www.mobistealth.com*)
  - MOBILE SPY (*http://www.mobile-spy.com*)
  - mSpy (*https://www.mspy.com*)
  - Highster mobile (*http://www.highstermobi.com*)
  - TeenSafe Monitor (*https://www.teensafe.com*)

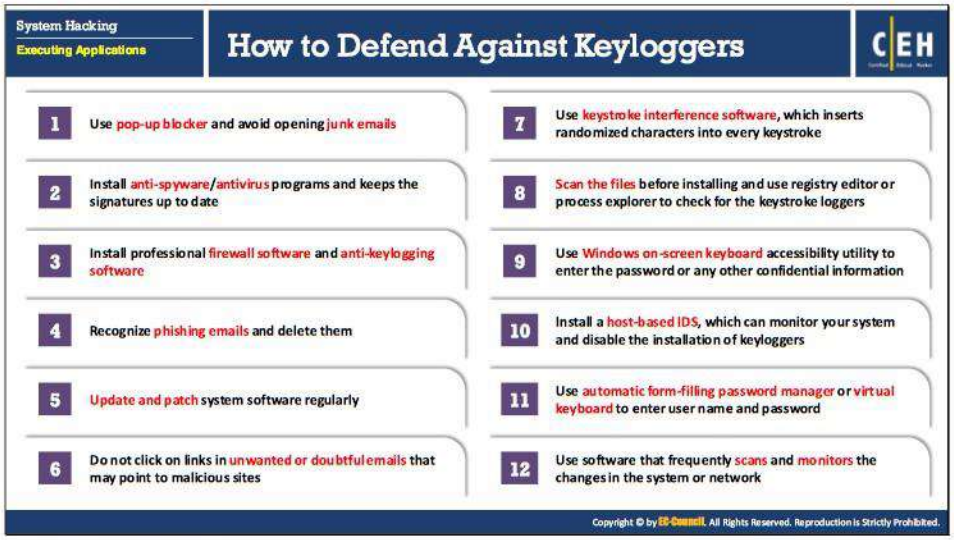
- **GPS Spyware**

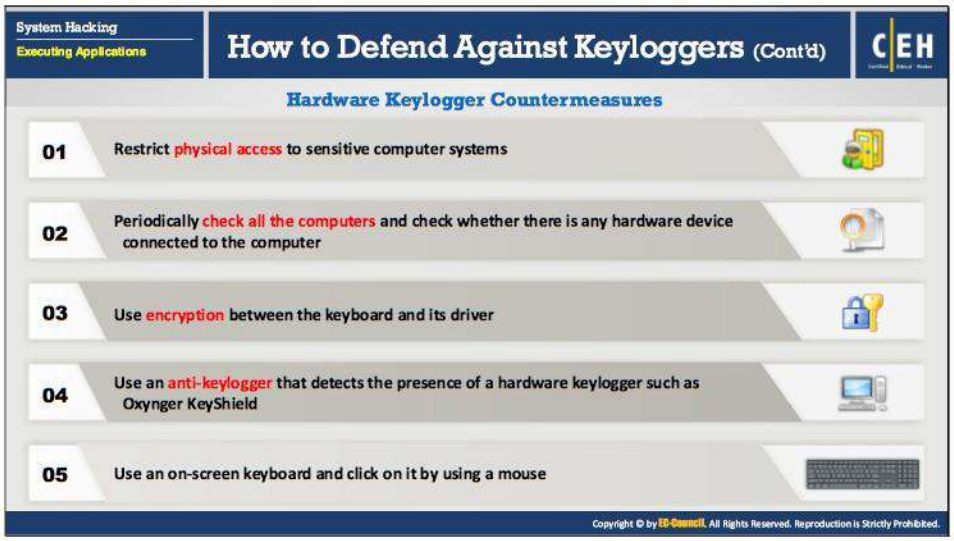
  There are various software programs that act as GPS spyware to trace the location of particular mobile devices. Attackers can also make use of the following GPS spyware software to track the location of target mobiles

  Some of the GPS spyware programs are listed below:

  - Spyera (*https://spyera.com*)
  - mSpy (*https://www.mspy.com*)
  - MOBILE SPY (*http://www.mobile-spy.com*)
  - MobiStealth (*http://www.mobistealth.com*)
  - FlexiSPY (*https://www.flexispy.com*)
  - THESPYPHONE (*https://www.thespyphone.com*)
  - EasyGPS (*http://www.easygps.com*)
  - Trackstick (*http://www.trackstick.com*)

- GPS TrackMaker Professional (*http://www.trackmaker.com*)
- GPS Tracking System (*http://www.spytechs.com*)
- Real Time GPS Tracker (*https://spyassociates.com*)
- SPY-SPOT GPS Tracker (*https://shop.spy-spot.com*)
- Linxup GPS Vehicle Tracker (*https://www.linxup.com*)
- SPYTEC GPS Tracker (*http://www.spytecinc.com*)





How to Defend Against Keyloggers

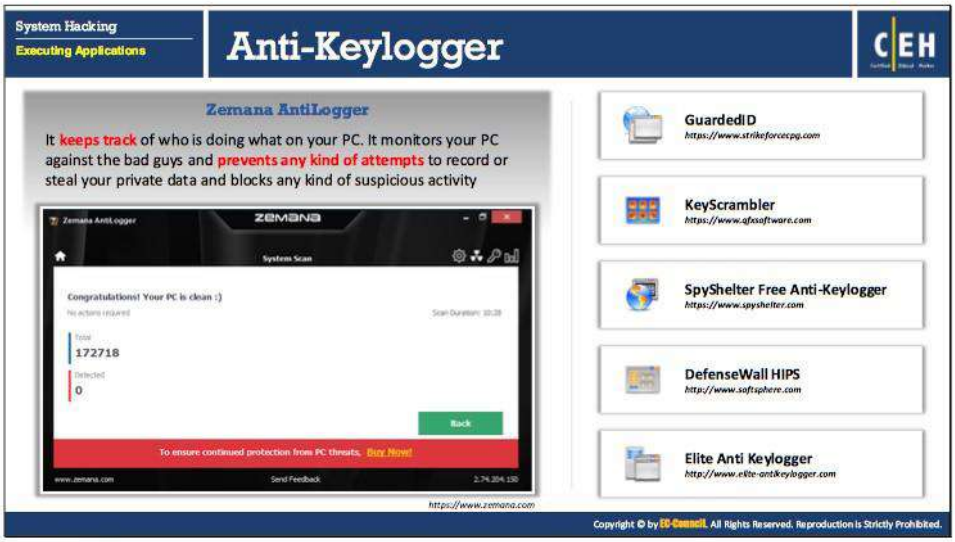
The following are some more ways to defend against keyloggers:

- Use pop-up blockers and avoid opening junk emails
- Install anti-spyware/antivirus programs and keep the signatures up to date
- Install professional firewall software and anti-keylogging software

- Recognize phishing emails and delete them
- Update and patch system software regularly to defend against keyloggers
- Do not click on links in unwanted or doubtful emails that may point to malicious sites
- Use keystroke interference software, which inserts randomized characters into every keystroke.
- Antivirus and antispyware software is able to detect any installed software, but it is better to detect these programs before installation. Scan the files thoroughly before installing them onto the computer and use a registry editor or process explorer to check for keystroke loggers.
- Use the Windows on-screen keyboard accessibility utility to enter the password or any other confidential information. You can maintain your information confidentially because you use mouse to enter any information such as passwords and credit card numbers into the keyboard, instead of typing the passwords using the keyboard.
- Use automatic form-filling password manager or a virtual keyboard to enter user names and passwords because they avoid exposure through keyloggers. This automatic form-filling password manager will remove the use of typing your personal, financial, or confidential details such as credit card numbers and passwords through keyboards.
- Keep your hardware systems secure in a locked environment and frequently check the keyboard cables for the attached connectors, USB port, and computer games such as the PS2 that have been used to install keylogger software.
- Use software that frequently scans and monitors the changes in the system or network.
- Install host-based IDS, which can monitor your system and disable the installation of keyloggers.

Hardware Keylogger Countermeasures

- Restrict physical access to sensitive computer systems
- Periodically check your keyboard interface to ensure that no extra components are plugged to the keyboard cable connector
- Use encryption between the keyboard and its driver
- Use an anti-keylogger that detects the presence of a hardware keylogger such as OxyngerKeyShield
- Use an on-screen keyboard and click on it by using a mouse



Anti-Keyloggers

Anti-keyloggers, also called anti-keystroke loggers, detect and disable keystroke logger software. Anti-keylogger's special design helps them to detect software keyloggers. Many large organizations, financial institutions, online gaming industries, as well as individuals use anti-keyloggers for protecting their privacy while using systems. This software prevents a keylogger from logging every keystroke typed by the victim and thus keeps all personal information safe and secure. An anti-keylogger scans a computer, detects, and removes keystroke logger software. If the software (anti-keylogger) finds any keystroke logging program on your computer, it immediately identifies and removes the keylogger, whether it is legitimate keystroke logging program or an illegitimate keystroke logging program.

Some of the anti-keyloggers detect the presence of hidden keyloggers by comparing all files in the computer against a signature database of keyloggers and searching for similarities. Other anti-keyloggers detect the presence of hidden keyloggers by protecting keyboard drivers and kernels from manipulation. A virtual keyboard or touchscreen makes the keystroke capturing job of malicious spyware or Trojan programs difficult. Anti-keyloggers secure your system from spyware, keyloggers.

- **Zemana AntiLogger**

  Source: *https://www.zemana.com*

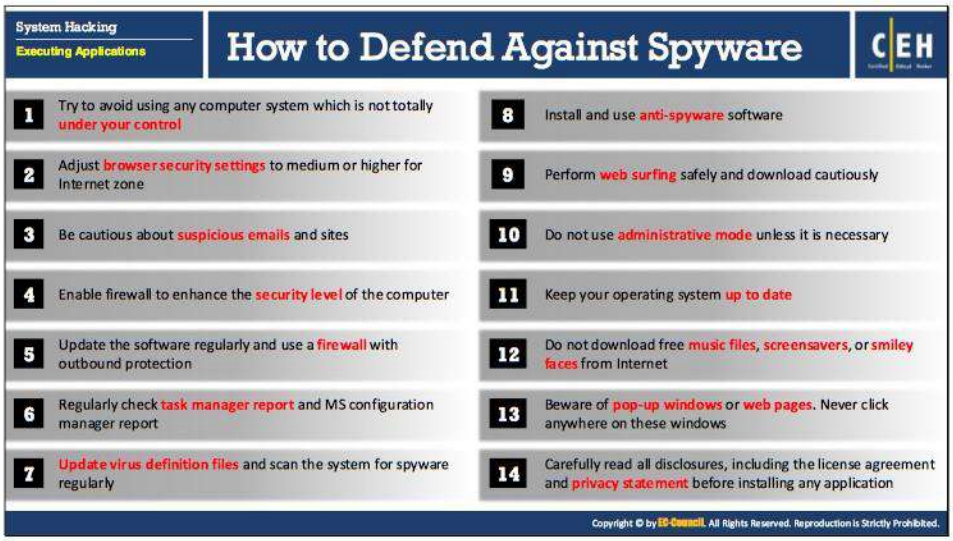
  Zemana AntiLogger is a software application that blocks hackers. It detects any attempts to modify your computer's settings, record your activities, hook to your PC's sensitive processes, or inject malicious code in your system. It protects your computer from keylogger and malware attacks, thereby protecting your identity. The AntiLogger detects the malware at the time it attacks your system rather than detecting it based on its signature fingerprint. It will prompt you if any malicious program is attempting to record

the keystrokes of your system, capture your screen, gain access to your clipboard, microphone, and webcam, or inject itself into any sensitive areas of your system.

Zemana Anti-logger provides protection against various threats such as SSL logger, webcam logger, Keyloggers, clipboard and screen logger, spyware, Trojans, and so on.

Some of the anti-keyloggers are listed below:

- GuardedID (*https://www.strikeforcecpg.com*)
- KeyScrambler (*https://www.qfxsoftware.com*)
- SpyShelter Free Anti-Keylogger (*https://www.spyshelter.com*)
- DefenseWall HIPS (*http://www.softsphere.com*)
- Elite Anti Keylogger (*http://www.elite-antikeylogger.com*)



How to Defend Against Spyware

Spyware is any malicious program installed onto a user's system without the user's knowledge and gathers confidential information such as personal data and access logs. Spyware comes from three basic sources: free downloaded software, email attachments, and websites that automatically install spyware when you browse them. Here are ways to defend against spyware:

- Try to avoid using any computer system which is not totally under your control.
- Never adjust your Internet security setting level too low because it provides many chances for spyware to install on your computer. So, always set your Internet browser security setting to either high or medium for protecting your computer from spyware.
- Don't open suspicious emails and file attachments received from unknown senders. There is a great likelihood that you will get a virus, freeware, or spyware on the computer. Don't open unknown websites present in spam mail messages, retrieved by search engines, or displayed in pop-up windows because they may mislead you to download spyware.
- Enable a Firewall to enhance the security level of your computer
- Update the software regularly and use a firewall with outbound protection
- Regularly check task manager report and MS configuration manager report
- Update virus definition files and scan the system for spyware regularly
- Install antispyware software. Antispyware protects against spyware. Antispyware is the first line of defense against spyware. This software prevents spyware installation on your system. It periodically scans your system and protects your system from spyware.

- Keep your operating system up to date.
  - Windows users should periodically perform the windows or Microsoft update.
  - For other users, using other operation systems or software products, refer to the information given by the operation system vendors, and take essential steps against any vulnerability identified.
- Perform web surfing safely and download cautiously
  - Before downloading any software, make sure that it is from a trusted website. Read the license agreement, security warning, and privacy statements associated with the software thoroughly to get a clear understanding before you download.
  - While downloading freeware or shareware from a Web site, ensure that the site is safe. Likewise, be cautious with software programs obtained through P2P file-swapping software. Before installing such programs, perform scan using anti-spyware software
- Do not use administrative mode unless it is necessary because it may execute malicious programs such as spyware in the administrator mode. As a result, attackers may take complete control over your system.
- Do not download free music files, screensavers, or smiley faces from the Internet because when you download such free programs, there is a possibility that spyware comes along with them invisibly.
- Beware of pop-up windows or web pages. Never click anywhere on the windows that display messages such as your computer may be infected, or that they can help your computer to run faster. When you click on such windows your system may get infected with spyware.
- Carefully read all disclosures, including the license agreement and privacy statement before installing any application
- Do not store personal or financial information on any computer system that is not totally under your control, such as in an Internet café.

Anti-Spyware

There are many anti-spyware applications available in the market, which scan your system and check for spyware such as malware, Trojans, dialers, worms, keyloggers, and rootkits, and remove them if found. Anti-spyware provides real-time protection by scanning your system at regular intervals, either weekly or daily. It scans to ensure the computer is free from malicious software.

- **SUPERAntiSpyware**

  Source: *http://www.superantispyware.com*

  SUPERAntiSpyware is a software application which can detect and remove spyware, adware, Trojan horses, rogue security software, computer worms, rootkits, parasites, and other potentially harmful software applications.

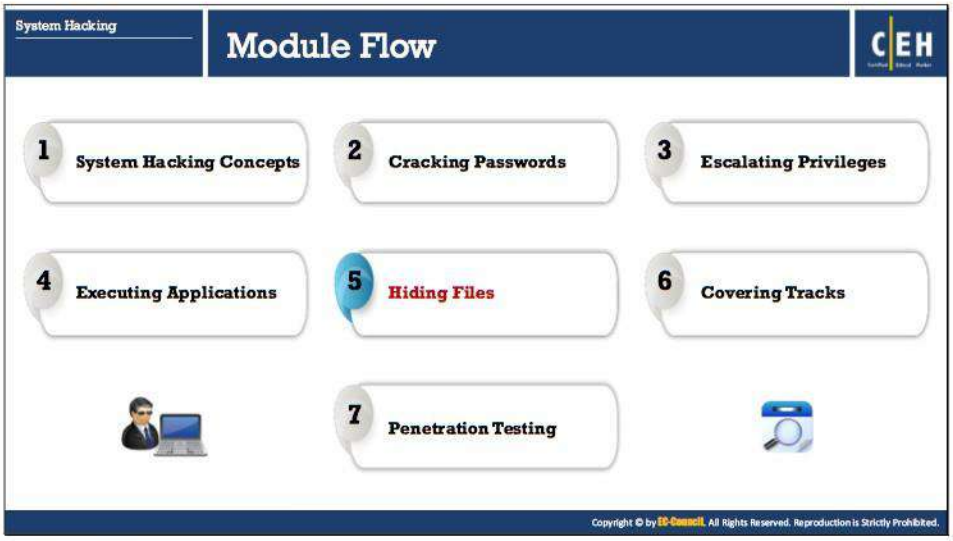
  Features:

  - Detect and Remove Spyware, Adware and Remove Malware, Trojans, Dialers, Worms, keyloggers, hijackers, Parasites, Rootkits, Rogue Security Products and many other types of threats.
  - Repair broken Internet Connections, Desktops, Registry Editing and more with our unique Repair System.
  - Real-time Blocking of threats. Prevent potentially harmful software from installing or re-installing.
  - Configure SUPERAntiSpyware to send you an e-mail with the results from specific actions.

- Schedule either quick, complete or custom scans Daily or Weekly to ensure your computer is free from harmful software. Remove spyware automatically.

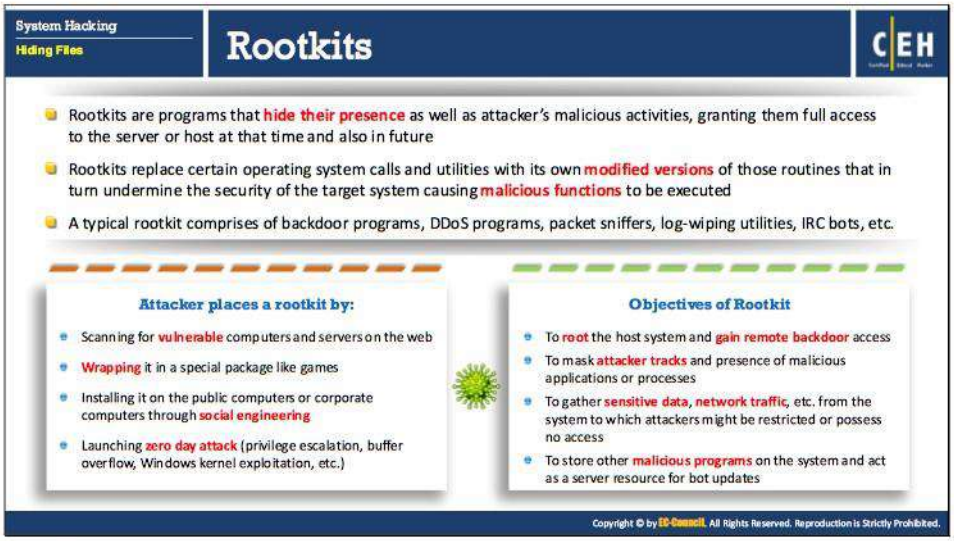
Some of the antispyware programs are listed below:

- Kaspersky Internet Security 2018 (*https://www.kaspersky.com*)
- SecureAnywhere Internet Security Complete (*https://www.webroot.com*)
- adaware antivirus free (*https://www.adaware.com*)
- MacScan (*https://www.securemac.com*)
- Norton AntiVirus Basic (*https://in.norton.com*)
- Spybot – Search & Destroy (*https://www.safer-networking.org*)
- SpyHunter (*https://www.enigmasoftware.com*)
- Malwarebytes for Windows (*https://www.malwarebytes.com*)
- Zemana Anitmalware (*https://www.zemana.com*)
- Hitman Pro (*https://www.hitmanpro.com*)
- Emsisoft Antimalware (*https://www.emsisoft.com*)
- Digital Care AntiVirus (*http://www.paretologic.com*)
- Spyware Terminator 2015 (*http://www.pcrx.com*)



Hiding Files

After an attacker has performed malicious operations (i.e., executed malicious applications) on the target system to get escalated access, the next step the attacker will take is to embed and hide his/her malicious programs. The attacker will hide their programs using Rootkits, NTFS Stream, and Steganography techniques, etc. in order to prevent the malicious program from protective applications such as Antivirus, Anti-malware, Anti-spyware applications, and so on installed on the target system. This allows the attacker to maintain future access to the system. Such a hidden malicious file provides direct access to the attacker without the victim's consent. This section will describe various techniques used by the attackers to hide his/her malicious file.



Rootkits

Rootkits are software programs aimed to gain access to a computer without detection. These are malware that help the attackers to gain unauthorized access to a remote system and perform malicious activities. The goal of the rootkit is to gain root privileges to a system. By logging in as the root user of a system, an attacker can perform any task such as installing software or deleting files, and so on. It works by exploiting the vulnerabilities in the operating system and applications. It builds a backdoor login process in the operating system by which the attacker can evade the standard login process.

Once the user enables root access, a rootkit may attempt to hide the traces of unauthorized access by modifying drivers or kernel modules and discarding active processes. Rootkits replace certain operating system calls and utilities with its own modified versions of those routines that in turn undermine the security of the target system by executing malicious functions. A typical rootkit comprises backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, and others.

All files contain a set of attributes. There are different fields in the file attributes. The first field determines the format of the file, if it is a hidden, archive, or read-only file. The other field describes the time of the file creation, access, as well as its original length. The functions **GetFileAttributesEx()** and **GetFileInformationByHandle()** are used for these purposes. ATTRIB.exe displays or changes the file attributes. An attacker can hide, or even change the attributes of a victim's files, so that the attacker can access them.

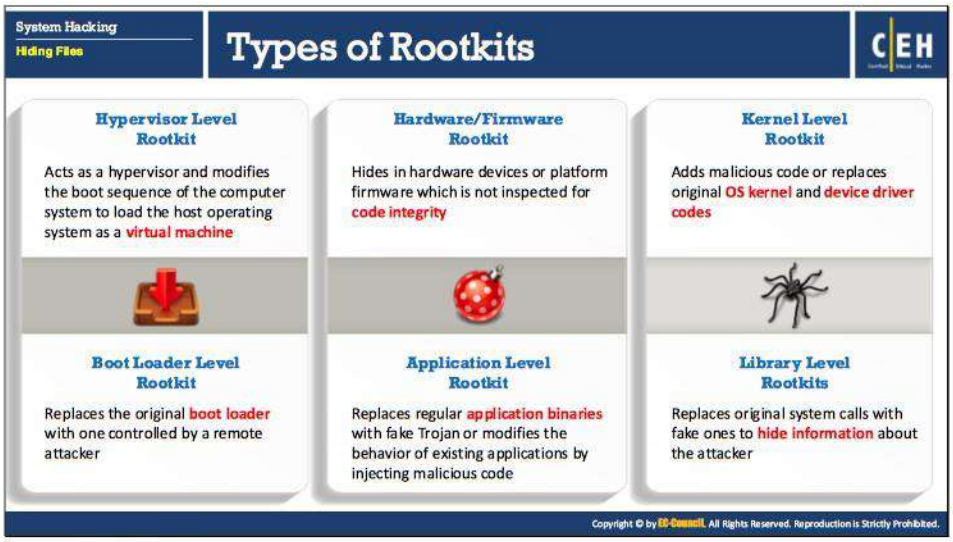
Attacker places a rootkit by:

- Scanning for vulnerable computers and servers on the web
- Wrapping it in a special package like games

- Installing it on the public computers or corporate computers through social engineering
- Launching zero-day attack (privilege escalation, Windows kernel exploitation, etc.)

Objectives of rootkit:

- To root the host system and gain remote backdoor access
- To mask attacker tracks and presence of malicious applications or processes
- To gather sensitive data, network traffic, etc. from the system to which attackers might be restricted or possess no access
- To store other malicious programs on the system and act as a server resource for bot updates



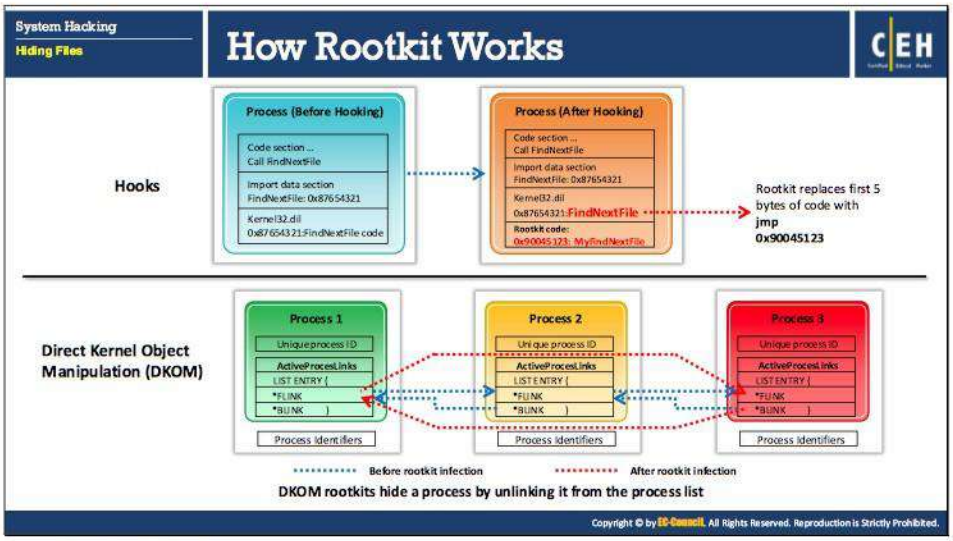
Types of Rootkits

A rootkit is a type of malware that can hide itself from the operating system and antivirus applications in the computer. This program provides the attackers with root-level access to the computer through the backdoors. These rootkits employ a range of techniques to gain control of a system. The type of rootkit influences the choice of attack vectors. Basically there are six types of rootkits available. They are:

- **Hypervisor Level Rootkit:** Attackers create Hypervisor level rootkits by exploiting hardware features such as Intel VT and AMD-V. These rootkits runs in Ring-1 and host the operating system of the target machine as a virtual machine and intercept all hardware calls made by the target operating system. This kind of rootkit works by modifying the system's boot sequence and gets loaded instead of the original virtual machine monitor.
- **Hardware/Firmware Rootkit:** Hardware/firmware rootkits use devices or platform firmware to create a persistent malware image in hardware, such as a hard drive, system BIOS, or network card. The rootkit hides in firmware as the users do not inspect it for code integrity. A firmware rootkit implies the use of creating a permanent delusion of rootkit malware.
- **Kernel Level Rootkit:** The kernel is the core of the operating system. Kernel level rootkit runs in Ring-0 with highest operating system privileges. These cover backdoors on the computer and are created by writing additional code or by substituting portions of kernel code with modified code via device drivers in Windows or loadable kernel modules in Linux. If the kit's code contains mistakes or bugs, kernel-level rootkits affect the stability of the system. These have the same privileges of the operating system;

hence, they are difficult to detect and intercept or subvert the operations of operating systems.

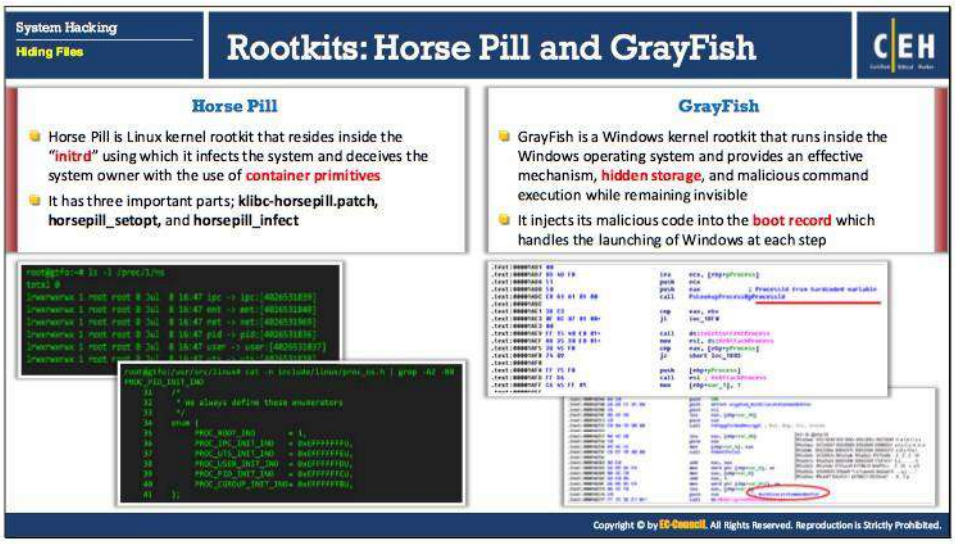
- **Boot Loader Level Rootkit:** Boot loader level (bootkit) rootkits function either by replacing or modifying the legitimate bootloader with another one. The boot loader level (bootkit) can activate even before the operating system starts. So, the boot-loader-level (bootkit) rootkits are serious threats to security because they can help in hacking encryption keys and passwords.
- **Application Level Rootkit:** Application level rootkit operates inside the victim's computer by replacing the standard application files (application binaries) with rootkits or by modifying behavior of present applications with patches, injected malicious code, and so on.
- **Library Level Rootkits:** Library level rootkits work higher up in the OS and they usually patch, hook, or supplant system calls with backdoor versions to keep the attacker unknown. They replace original system calls with fake ones to hide information about the attacker.



How Rootkit Works

System hooking is a process of changing and replacing the original function pointer with the pointer provided by the rootkit in stealth mode. Inline function hooking is a technique where a rootkit changes some of the bytes of a function inside the core system DLLs (kernel32.dll and ntdll. dll), placing an instruction so that any process calls hit the rootkit first.

Direct Kernel Object Manipulation (DKOM) rootkits are able to locate and manipulate the "system" process in kernel memory structures and patch it. This can also hide processes and ports, change privileges, and misguide the Windows event viewer without any problem by manipulating the list of active processes of the operating system, altering data inside the PROCESS IDENTIFIERS structures. It has an ability to obtain read/write access to the \Device\Physical Memory object. It hide a process by unlinking it from the process list.



Rootkits: Horse Pill and Gray Fish

The following are some of the popular rootkits:

- **Horse Pill**

  Source: *http://www.pill.horse*

  Horse Pill is a PoC of a ramdisk based containerizing root kit. It resides inside the initrd, and prior to the actual init running, it puts it into a mount and pid namespace that allows it to run covert processes and covert storage. This also allows it run covert networking systems, such as dns tunnels.

  It has three important moving parts:

  - **klibc-horsepill.patch**

    This is a patch to klibc, which provides run-init, which on modern Ubuntu systems runs the real init, systemd. This patches in the rootkit functionality, making a malicious run-init. This binary has a new section called DNSCMDLINE, which provides the command line options to dnscat, which is bundled within the patch.

  - **horsepill_setopt**

    This script takes in command-line arguments and puts them into the section referred to above.

  - **horsepill_infect**

    This will take the file to splat over run-init while assembling ramdisks as a command line argument. It then calls update-initramfs and splats over the run-init as the ramdisks is being assembled.

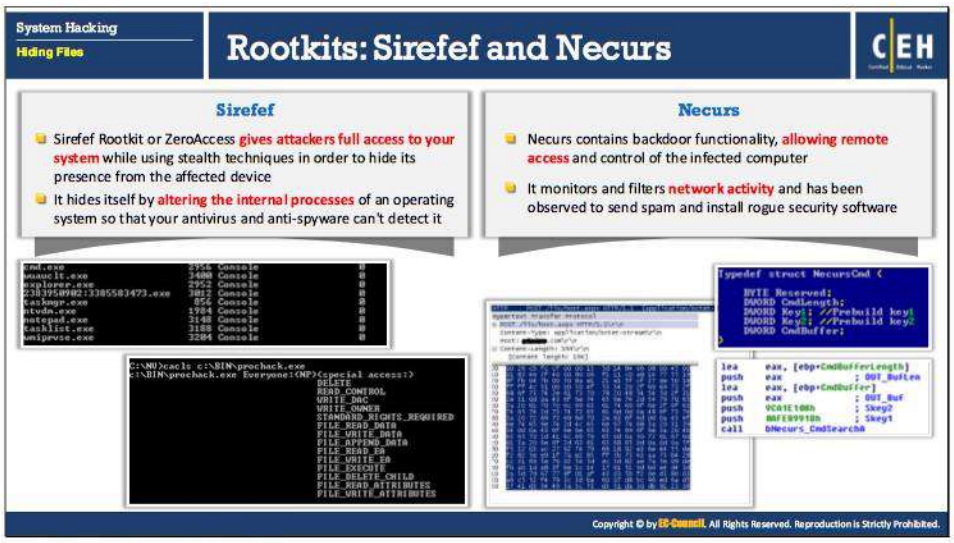
- **GrayFish Rootkit**

  Source: *http://artemonsecurity.blogspot.in*

  GrayFish is a Windows kernel rootkit that runs inside the Windows operating system and provides an effective mechanism, hidden storage and malicious command execution while remaining invisible. It injects its malicious code into the boot record which handles the launching of Windows at each step. It implements its own Virtual File System (VFS) to store the stolen data and its own auxiliary information. If we run rootkit driver on a machine and next scan it with various anti-rootkits, we will see no suspicious activity. This means that by default the rootkit sets no hooks on Windows kernel functions like other rootkits. The rootkit also does not register any callback functions, for example, on process creation or modules loading.

  GrayFish doesn't explore Windows kernel mode to monitor system's activity or hiding files on disk. At the same time, it contains the code for patching Windows kernel functions. This code can be activated later.

  Like other rootkits, GrayFish contains code for code/data injection into processes with help of ZwOpenProcess/PsLookupProcessByProcessId/KeStackAttachProcess. While this rootkit works with user mode memory during injection, it calls interesting system function - MmSecureVirtualMemory. It receives all its instructions from user mode client.



Rootkits: Sirefef and Necurs

- **Sirefef**

  Source: *https://www.lifewire.com*

  The Sirefef malware (aka ZeroAccess) can take on many forms. It is considered to be a multi-component family of malware, which means that it can be implemented in a variety of different ways such as a rootkit, virus, or a Trojan horse.

  It gives attackers full access to your system while using stealth techniques in order to hide its presence from the affected device. It hides itself by altering the internal processes of an operating system so that your antivirus and anti-spyware can't detect it. It includes a sophisticated self-defense mechanism which terminates any security-related processes that attempt to access it.

  Sirefef is a severe malware that can cause damage to your computer in a variety of ways. Once installed, Sirefef can make lasting modifications to your computer's security settings and can be difficult to remove.

  After installation in the system, it has the capability to do the following tasks:

  - Stops Windows Firewall
  - Stops Windows Defender Service
  - Contacts remote hosts
  - Changes Internet Browser settings
  - Creates a folder to store other malware

- **Necurs**

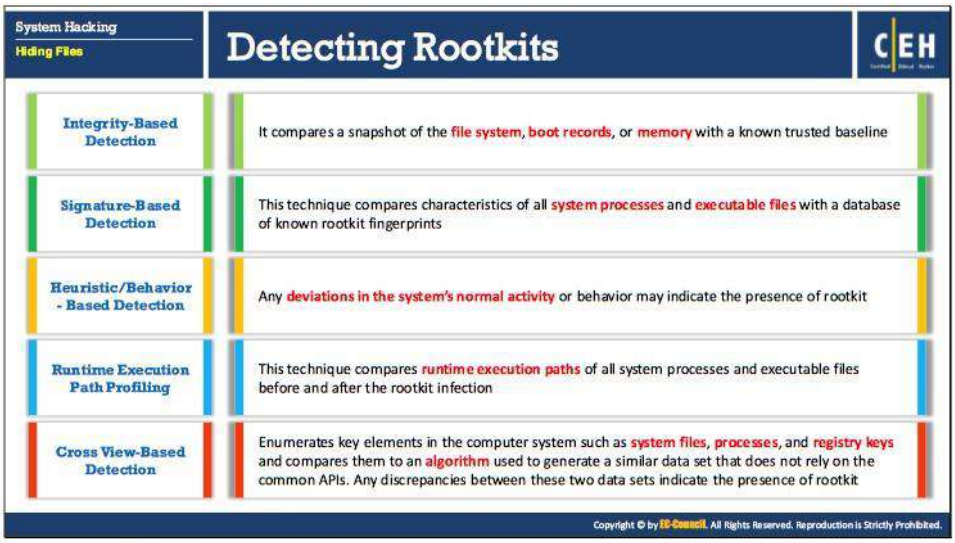
  Source: *https://www.f-secure.com*

  Necurs is a kernel-mode driver component that can be used by an attacker (or added as a component to another malicious program) to perform unauthorized actions to take control of an operating system, without alerting the system's security mechanisms. Necurs contains backdoor functionality, allowing remote access and control of the infected computer. It monitors and filters network activity and has been observed to send spam and install rogue security software. It enables further compromise by providing the functionality to:

  - Download additional malware
  - Hide its components
  - Stop security applications from functioning

Listed below are some of the popular rootkits:

- WingBird Rootkit
- Avatar
- Azazel
- ZeroAccess
- Alureon



Detecting Rootkits

We have seen how attackers make use of various rootkits to hide files and their presence on the target system. Now it's time to discuss various detection methods for the rootkit detection from a security perspective. Basically, types of rootkit detection techniques are signature, heuristic, integrity, cross view-based, and Runtime Execution Path Profiling.

- **Integrity-Based Detection**

  Integrity based detection can be regarded as a substitute to both signatures and heuristics based detection. Initially, the user runs tools such as Tripware, AIDE, etc. on a clean system. These tools create a baseline of clean system files and store them in a database. Integrity-based detection functions by comparing a current file system, boot records, or memory snapshot with that trusted baseline. They notify the evidence or presence of malicious activity based on the dissimilarities between the current and baseline snapshots.

- **Signature-Based Detection**

  Signature-based detection methods work as a rootkit fingerprint. It compares characteristics of all system processes and executable files with a database of known rootkit fingerprints. You can compare the sequence of bytes from a file compared with another sequence of bytes that belong to a malicious program. The method mostly scans the system files. It can easily detect invisible rootkits by scanning the kernel memory. The success of signature-based detection is less due to the rootkit's tendency to hide files by interrupting the execution path of the detection software.

- **Heuristic/Behavior-Based Detection**

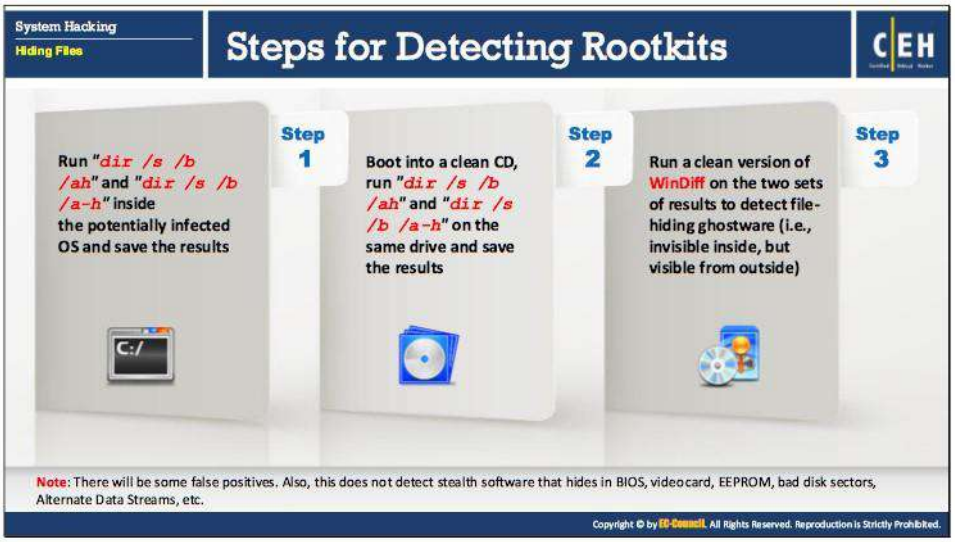
  Heuristic detection works by identifying deviations in normal operating system patterns or behaviors. This kind of detection is also known as behavioral detection. Heuristic detection is capable of identifying new, previously unidentified rootkits. This ability lies in being able to recognize deviants in "normal" system patterns or behaviors. Execution path hooking is one such deviant that causes heuristic-based detectors to identify rootkits.

- **Runtime Execution Path Profiling**

  The Runtime Execution Path Profiling technique compares runtime execution path profiling of all system processes and executable files. The rootkit adds new code near to a routine's execution path to destabilize it. The method hooks a number of instructions executed before and after a certain routine, as it can be significantly different.

- **Cross View-Based Detection**

  Cross view-based detection techniques function by assuming the operating system has been subverted in some way. This enumerates the system files, processes, and registry keys by calling common APIs. The tools compare the gathered information with the data set obtained through the use of an algorithm traversing through the same data. This detection technique relies upon the fact that the API hooking or manipulation of kernel data structure taints the data returned by the operating system APIs, with the low-level mechanisms used to output the same information free from DKOM or hook manipulation.



Steps for Detecting Rootkits

Source: *http://searchenterprisedesktop.techtarget.com*

There are many tools available in the market to detect the presence of rootkits on the target system. But sometimes tools come up short as the malware writers always find ways to counter these automated rootkit detectors and some of their latest efforts are able to even evade it. So, it is better to detect the rootkit manually. Manual detection of rootkits requires time, patience, perseverance, and expertise.

Examine the file system and Registry of the system to detect the rootkits manually.

- **Steps to detect rootkits by examining file system**
  1. Run "`dir /s /b /ah`" and "`dir /s /b /a-h`" inside the potentially infected OS and save the results
  2. Boot into a clean CD, run "`dir /s /b /ah`" and "`dir /s /b /a-h`" on the same drive and save the results
  3. Run a clean version of **WinDiff** on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)
- **Steps to detect rootkits by examining the registry**
  1. Run **regedit.exe** from inside the potentially infected operating system.
  2. Export **HKEY_LOCAL_MACHINE\SOFTWARE** and **HKEY_LOCAL_MACHINE\SYSTEM** hives in text file format.
  3. Boot into a **clean CD** (such as **WinPE**).
  4. Run **regedit.exe**.

5. Create a new key such as **HKEY_LOCAL_MACHINE\Temp**.
6. Load the Registry hives named Software and System from the suspect operating system. The default location will be **c:\windows\system32\config\software** and **c:\windows\system32\config\system**.
7. Export these Registry hives in text file format. (The Registry hives are stored in binary format and Steps 6 and 7 convert the files to text.)
8. Launch **WinDiff** from the CD, and compare the two sets of results to detect file-hiding malware (i.e., invisible inside, but visible from outside).

Note: There can be some false positives. Also, this does not detect stealth software that hides in BIOS, video card EEPROM, bad disk sectors, Alternate Data Streams, and so on.

How to Defend against Rootkits

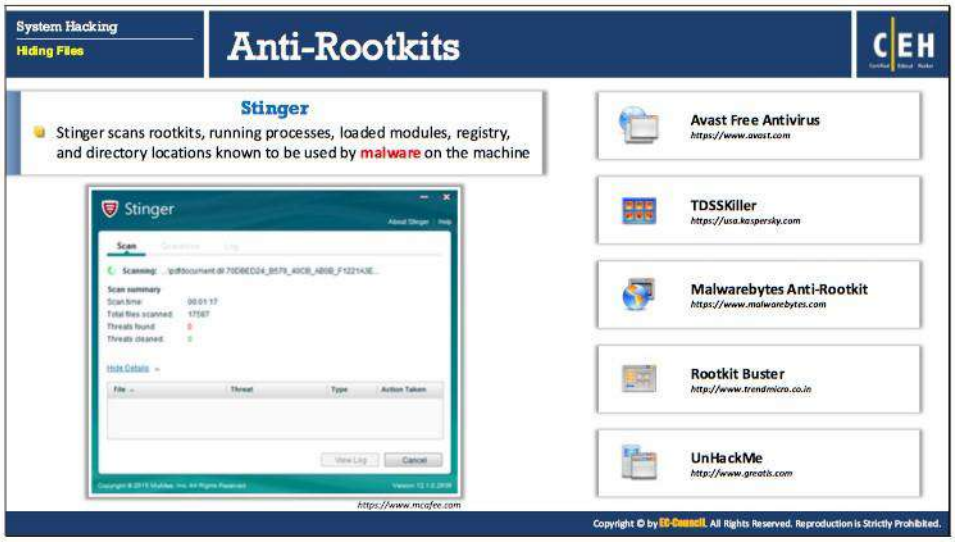
A common feature of these rootkits is that the attacker requires administrator access to the target system. The initial attack that leads to this access is often noisy. Monitor the excess network traffic that arises in the face of a new exploit. It goes without saying that log analysis is a part and parcel of risk management. The attacker may have shell scripts or tools that can help him or her cover his or her tracks, but surely there will be other telltale signs that can lead to proactive countermeasures, not just reactive ones.

A reactive countermeasure is to back up all critical data excluding the binaries, and go for a fresh clean installation from a trusted source. One can do code check summing as a good defense against tools like rootkits. MD5sum.exe can fingerprint files and note integrity violations when changes occur. To defend against rootkits, use integrity checking programs for critical system files.

A few techniques adopted to defend against rootkits are:

- Reinstall OS/applications from a trusted source after backing up the critical data
- Well-documented automated installation procedures need to be kept
- Perform kernel memory dump analysis to determine the presence of rootkits
- Harden the workstation or server against the attack
- Educate staff not to download any files/programs from untrusted sources
- Install network and host-based firewalls and check frequent updates
- Ensure the availability of trusted restoration media
- Update and patch operating systems and applications

- Verify the integrity of system files regularly using cryptographically strong digital fingerprint technologies
- Update antivirus and anti-spyware software regularly
- Keep the signatures of anti-malware up to date
- Avoid logging into an account with administrative privileges
- Adhere to the least privilege principle
- Ensure that the chosen antivirus software possesses rootkit protection
- Do not install unnecessary applications and also disable the features and services not in use
- Refrain from engaging in dangerous activities on the internet
- Close any unused ports
- Periodically scans the local system using Host-Based Security Scanners
- Harden the security of system such as use strong password, so that an attacker will not get root access on the system to install rootkits



Anti-Rootkits

The following anti-rootkits can help you to remove various types of malware such as rootkits, viruses, Trojan, and worms from your system. You can download or purchase anti-rootkit software from their home sites and install it on your PC to get protection from malware especially from rootkits.

- **Stinger**

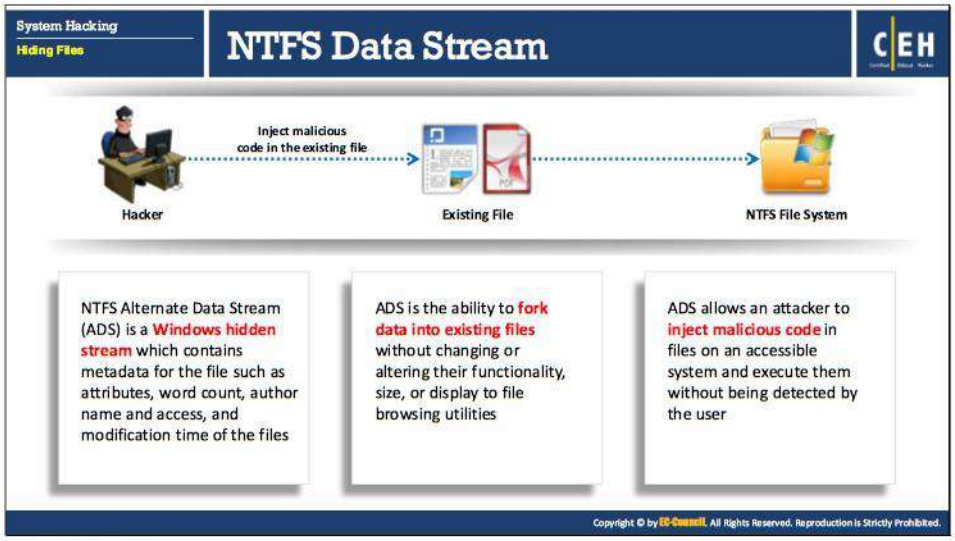
  Source: *https://www.mcafee.com*

  McAfee Stinger is a standalone utility used to detect and remove specific viruses. It helps administrators and users when dealing with an infected system. Stinger performs rootkit scanning, and scan performance optimizations. It detects and removes threats identified under the "Threat List" option under advanced menu options in the Stinger application.

A few more important anti-rootkits are:

- Avast Free Antivirus (*https://www.avast.com*)
- TDSSKiller (*https://usa.kaspersky.com*)
- Malwarebytes Anti-Rootkit (*https://www.malwarebytes.com*)
- Rootkit Buster (*http://www.trendmicro.co.in*)
- UnHackMe (*http://www.greatis.com*)
- Virus Removal Tool (*https://www.sophos.com*)
- F-Secure Anti-Virus (*https://www.f-secure.com*)

- Avira Free Antivirus (*https://www.avira.com*)
- SanityCheck (*http://www.resplendence.com*)
- Webroot (*https://www.webroot.com*)
- GMER (*http://www.gmer.net*)



NTFS Data Stream

NTFS is the file system that stores any file with the help of two data streams called NTFS data streams along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions, and the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

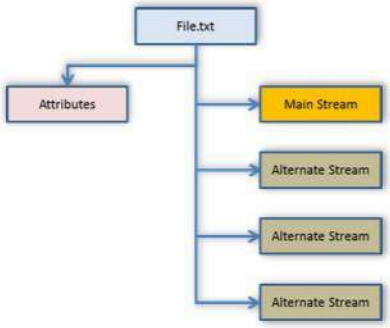
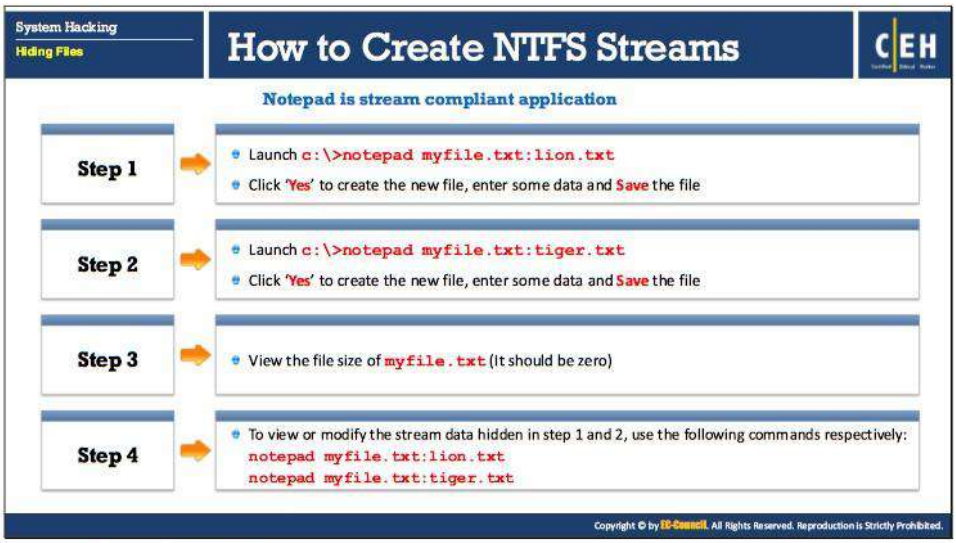


FIGURE 6.3: NTFS Data Stream

Alternate Data Stream (ADS) is any kind of data attached to a file, but not in the file on an NTFS system. The Master File Table of the partition will contain a list of all the data streams that a file contains, and where their physical location on the disk is. Therefore, alternate data streams are not present in the file, but attached to it through the file table. NTFS Alternate Data Stream (ADS) is a Windows hidden stream that contains metadata for the file such as attributes, word count, author name, and access and modification time of the files.

ADS is the ability to fork data into existing files without changing or altering their functionality, size, or display to file browsing utilities. ADS allows an attacker to inject malicious code in files on an accessible system and execute them without being detected by the user. ADSs provide attackers with a method of hiding rootkits or hacker tools on a breached system and allow user to execute them while hiding from the system's administrator.

Files with ADS are impossible to detect using native file browsing techniques like the command line or Windows Explorer. After attaching an ADS file to the original file, the size of the file will show as the original size of the file regardless of the size of the ADS added file. The only indication that the file was changed is the modification timestamp, which can be relatively innocuous.



How to Create NTFS Streams

Using NTFS data steam, an attacker can almost completely hide files within the system. It is easy to use the streams but the user can only identify it with specific software. Explorer can display only the root files; it cannot view the streams linked to the root files and cannot define the disk space used by the streams. As such, if a virus implants itself into ADS, it is unlikely that usual security software will identify it.

When the user reads or writes a file, it manipulates the main data stream by default.

Let's see how to create an alternate data stream for a file. Alternate data streams follow the syntax: "filename.ext:alternateName"

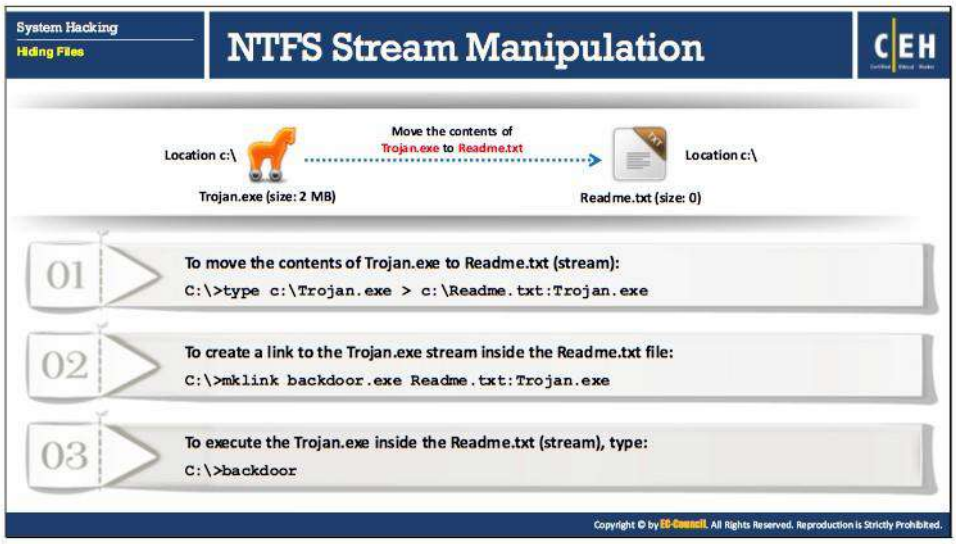
Steps to create NTFS Streams:

1. Launch `c:\>notepad myfile.txt:lion.txt` and click **'Yes'** to create the new file, enter some data and **Save** the file
2. Launch `c:\>notepad myfile.txt:tiger.txt` and click **'Yes'** to create the new file, enter some data and **Save** the file
3. View the file size of `myfile.txt` (It should be zero)
4. To view or modify the stream data hidden in step 1 and 2, use the following commands respectively:

   `notepad myfile.txt:lion.txt`

   `notepad myfile.txt:tiger.txt`

Note: Notepad is a stream compliant application. You should not use alternate streams for storing any critical information.



NTFS Stream Manipulation

You can manipulate NTFS Streams to hide a malicious file in other files, such as text files, by doing the following:

- **Hiding Trojan.exe (malicious program) into Readme.txt (stream):**

  Use the following command to move the contents of Trojan.exe to Readme.txt (stream):

  `c:\>type c:\Trojan.exe >c:\Readme.txt:Trojan.exe`

  The "type" command hides file in an Alternate Data Streams (ADS) behind an existing file. The colon (:) operator tells the command to create or use an ADS.

- **Creating a link to the Trojan.exe stream inside the Readme.txt file:**

  After hiding the file Trojan.exe behind the Readme.txt file, you need to create a link to launch the Trojan.exe file from the stream. This creates a shortcut for Trojan.exe in the stream.

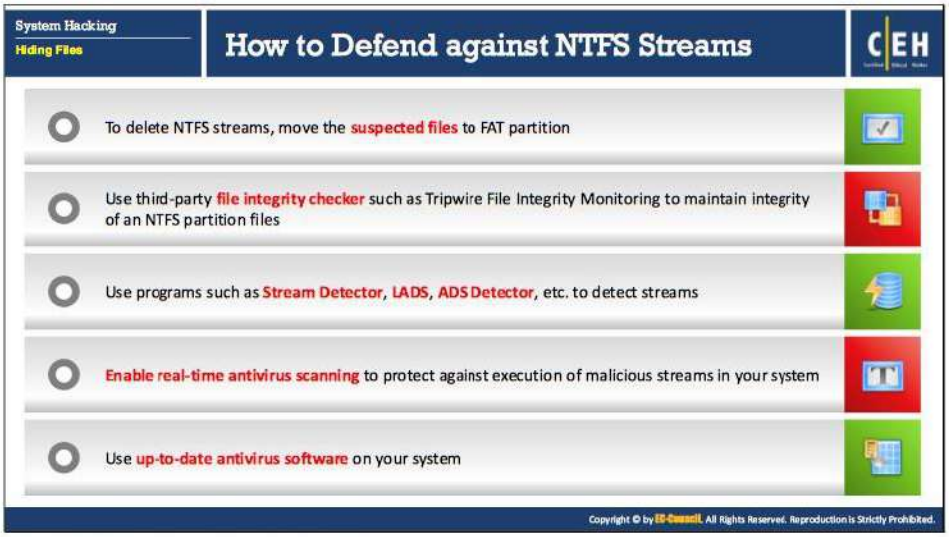
  `C:\>mklink backdoor.exe Readme.txt:Trojan.exe`

- **Executing the Trojan:**

  Type `C:\>backdoor` to run the Trojan that you have hidden behind Readme.txt. Here, the backdoor is the shortcut created in the previous step, which on execution installs the Trojan.

Note: Use notepad to read the hidden file.

For example, the command `C:\>notepad sample.txt:secret.txt`creates the secret.txt stream behind the sample.txt file.



How to Defend against NTFS Streams

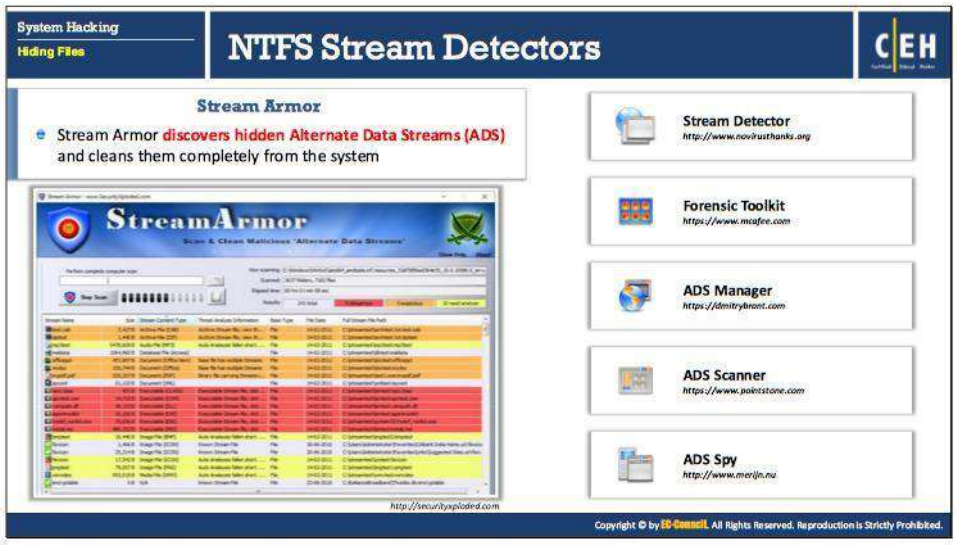
You should do the following to defend against malicious NTFS streams:

- To delete hidden NTFS streams, move the suspected files to FAT partition
- Use third-party file integrity checker such as Tripwire File Integrity Monitor to maintain integrity of NTFS partition files against unauthorized ADS
- Use third-party utilities such as EventSentry or adslist.exe to show and manipulate hidden streams
- Avoid writing important or critical data to alternate data streams
- Use up-to-date antivirus software on your system.
- Enable real-time antivirus scanning to protect against execution of malicious streams
- Use file-monitoring software such as Stream Detector (*http://www.novirusthanks.org*) and ADS Detector (*https://sourceforge.net/projects/adsdetector/?source=directory*)to help detect creation of additional or new data streams.

You should use LADS(*https://www.aldeid.com/wiki/LADS*) software as a countermeasure for NTFS streams. The latest version of lads.exe is GUI-based and reports the existence of Alternate Data Streams. It searches for either single or multiple streams, reports the presence of ADSs, and provides the full path and length of each ADS found.

Other means include copying the cover file to a FAT partition, and then moving it back to the NTFS. Where FAT file systems do not support Alternate Data Streams, this will effectively remove them from the original file.

LNS (*http://ntsecurity.nu/toolbox/lns*) and Forensic Toolkit (*https://www.mcafee.com*) are another tools used to detect NTFS streams. This tool is useful in forensic investigation.



NTFS Stream Detectors

There are various NTFS Stream Detectors available on the market. You can detect suspicious streams with the following NTFS stream detectors. You can download and install these stream detectors from their home sites.

- **Stream Armor**

  Source: *http://securityxploded.com*

  Stream Armor is a tool used to discover hidden Alternate Data Streams (ADS) and clean them completely from your system. Its advanced auto analysis, coupled with an online threat verification mechanism, helps you eradicate any ADSs.

  It has a multi-threaded ADS scanner that recursively scans the entire system to quickly uncover all hidden streams. "System" displays all discovered streams using a specific color pattern, according to the threat level, which makes it easy to distinguish suspicious and normal streams. "Forensic Analysis" uncovers hidden documents/images/audio/video/database/archive files in the ADSs.

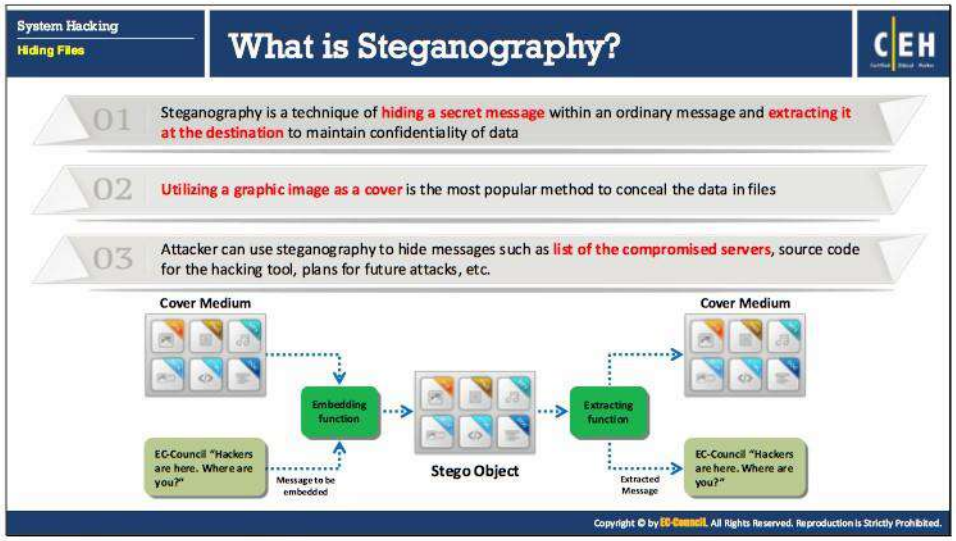
  Features:

  - Stream file type detection analyzes the internal content of files to detect the real file type rather than just going by the file extension.
  - Sophisticated "Auto Threat Analysis" is based on heuristic technology for identifying anomaly in the discovered streams based on the characteristics and patterns.
  - Save the selected stream file content to a disk, or USB drive or DVD for further analysis.

- Execute/Run the selected executable stream file for analyzing its malicious nature in virtual environments such as VMware.

Some of the NTFS stream detectors are listed below:

- Stream Detector (*http://www.novirusthanks.org*)
- Forensic Toolkit (*https://www.mcafee.com*)
- ADS Manager (*https://dmitrybrant.com*)
- ADS Scanner (*https://www.pointstone.com*)
- ADS Spy (*http://www.merijn.nu*)
- Streams (*https://docs.microsoft.com*)
- AlternateStreamView (*http://www.nirsoft.net*)
- ADS Detector (*https://sourceforge.net*)
- GMER (*http://www.gmer.net*)
- NTFS-Streams: ADS manipulation tool (*https://sourceforge.net*)



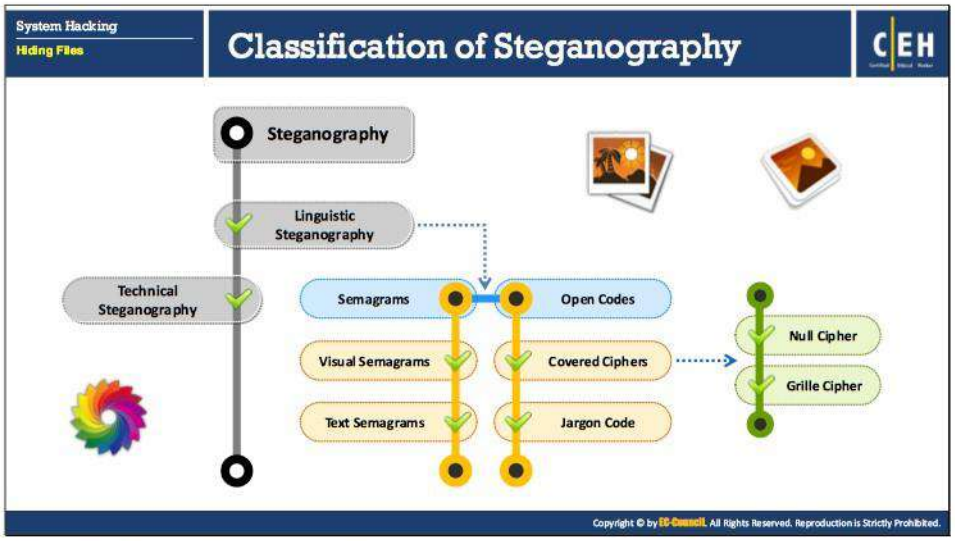
What is Steganography?

One of the shortcomings of various detection programs is their primary focus on streaming text data. What if an attacker bypasses normal surveillance techniques and still steals or transmits sensitive data? In a typical situation, after an attacker manages to get inside a firm as a temporary or contract employee, he surreptitiously seeks out sensitive information. While the organization may have a policy that does not allow removable electronic equipment in the facility, a determined attacker can still find ways to do so using techniques such as steganography.

Steganography refers to the art of hiding data "behind" other data without the target's knowledge. Thus, Steganography hides the existence of the message. It replaces bits of unused data into the usual files such as graphic, sound, text, audio, video, etc. with some other surreptitious bits. The hidden data can be plaintext or cipher text, or it can be an image. Utilizing a graphic image as a cover is the most popular method to conceal the data in files. Unlike encryption, detection of steganography is not easy. Thus, steganography techniques tempt attackers to use it for malicious purposes.

For example, attackers can hide a keylogger inside a legitimate image; so when the victim clicks on the image, the keylogger captures the victim's keystrokes.

Attackers also use steganography to hide information when encryption is not feasible. In terms of security, it hides the file in an encrypted format, so that even if the attacker decrypts it, the message will remain hidden. Attackers can insert information such as: source code for a hacking tool, list of compromised servers, plans for future attacks, communication and coordination channel, etc.



Classification of Steganography

Steganography is classified into two areas, according to technique: technical and linguistic. **Technical** steganography hides a message using scientific methods, whereas **linguistic** steganography hides it in a **carrier**; the specific medium used to communicate or transfer messages or files. The steganography **medium** is the combination of hidden message, carrier, and steganography key.

Technical Steganography

Technical steganography uses invisible ink, microdots, and other means, using physical or chemical methods to hide the message's existence. It is almost difficult to categorize all the methods by which these goals are achieved, but some of these include:

- **Invisible Ink**

  Invisible ink, or "security ink," is one of the methods of technical steganography. It is used for invisible writing with colorless liquids and can later be made visible by certain pre-negotiated manipulations such as lighting or heating. For example, if you use onion juice and milk to write a message, the writing will be invisible, but when heat is applied, it turns brown and the message becomes visible.

  Applications of Invisible ink:

  - Used in espionage
  - Anti-counterfeiting
  - Property marking
  - Hand stamping for venue re-admission
  - Marking for the purpose of identification in manufacturing

- **Microdots**

  A microdot is text or an image considerably condensed in size (with the help of a reverse microscope), up to one page in a single dot, to avoid detection by unintended recipients. Microdots are usually circular, about one millimeter in diameter, but are changeable into different shapes and sizes.

- **Computer-Based Methods**

  A computer-based method makes changes to digital carriers to embed information foreign to the native carriers. Communication of such information occurs in the form of text, binary files, disk and storage devices, and network traffic and protocols, and can alter the software, speech, pictures, videos or any other digitally represented code for transmission.

  Computer-based Steganography Techniques

  Classification of steganography techniques includes six groups, according to the cover modifications applied in the embedding process. They are:

  - **Substitution Techniques:** In this technique, the attacker tries to encode secret information by substituting the insignificant bits with the secret message. If the receiver has the knowledge of the places where the attacker embeds secret information, then she/he can extract the secret message.
  - **Transform Domain Techniques:** The transform domain technique of steganography hides the information in significant parts of the cover image such as cropping, compression, and some other image processing areas. This makes it tougher for attacks. One can apply the transformations to blocks of images or over the entire image.
  - **Spread Spectrum Techniques:** This technique is less susceptible to interception and jamming. In this technique, communication signals occupy more bandwidth than required to send the information. The sender increases the band spread by means of code (independent of data), and the receiver use a synchronized reception with the code to recover the information from the spread spectrum data.
  - **Statistical Techniques:** This technique utilizes the existence of **"1-bit"** steganography schemes by modifying the cover in such a way that, when transmission of a **"1"** occurs, some of the statistical characteristics change significantly. In other cases, the cover remains unchanged, to distinguish between the modified and unmodified covers. The theory of hypothesis from mathematical statistics helps in extraction.
  - **Distortion Techniques:** In this technique, user implements a sequence of modifications to the cover in order to get a stego-object. The sequence of modifications is such that it represents the transformation of a specific message. The decoding process in this technique requires knowledge about the original cover. The receiver of the message can measure the differences between the original cover and the received cover to reconstruct the sequence of modifications.

- **Cover Generation Techniques:** In this technique, the development of digital objects is to cover secret communication. When this information is encoded, it ensures the creation of a cover for secret communication.

Linguistic Steganography

This type steganography hides the message in the carrier another file. Further classification of linguistic steganography includes Semagrams and Open Codes.

- **Semagrams**

  Semagrams involve the steganography technique that hides information with the help of signs or symbols. In this technique, the user embeds some objects or symbols in the data to change the appearance of data to a predetermined meaning. The classification of semagrams is as follows:

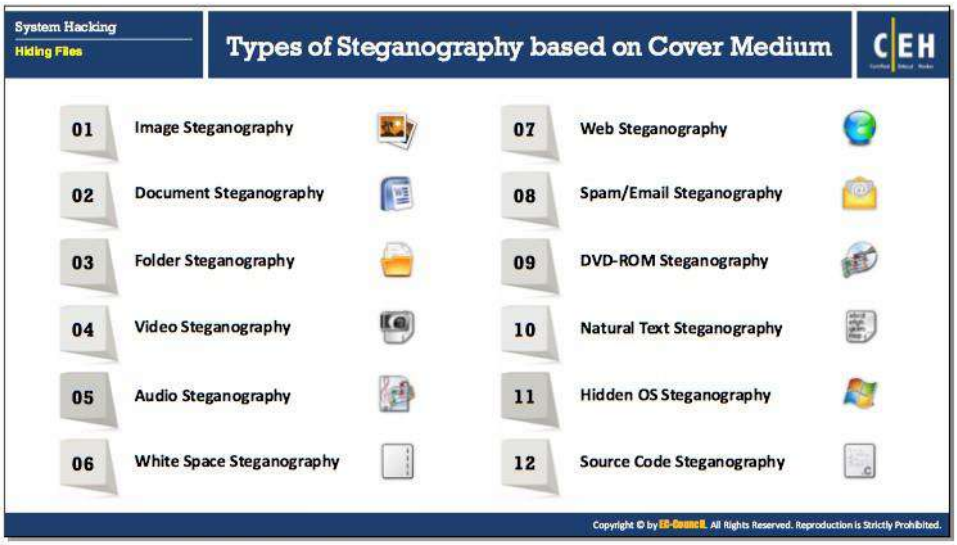
  - **Visual Semagrams:** This technique of steganography hides information in drawing, painting, letter, music or a symbol.
  - **Text Semagrams:** A text semagram hides the text message by converting or transforming its look and appearance of the carrier text message, such as changing font sizes and styles, adding extra spaces as white spaces in the document, and different flourishes in letters or handwritten text.

- **Open Codes**

  Open code hides the secret message in a legitimate carrier message specifically designed in a pattern on a document that is unclear to the average reader. The carrier message, sometimes also known as the overt communication and the secret message, is the covert communication. The open code technique consists of two main groups: jargon codes and covered ciphers.

  - **Jargon Codes:** In this type of steganography, a certain language is used that can be understood by a particular group of people for whom it is addressed, while being meaningless to others. A jargon message is like a substitution cipher in many respects, but instead of replacing individual letters, the words themselves are changed. An example of the jargon code is "**cue**" code. A *cue* is a word that appears in text and then transports the message.
  - **Covered Ciphers:** The technique hides the message in a carrier medium visible to everyone. This type of message can be extracted by any person with knowledge of the method used to hide it. Further classification of cover ciphers includes null ciphers and grille ciphers.
    - **Null ciphers:** A technique used to hide the message with a large amount of useless data. Mix the original data with the unused data in any order diagonally, vertically, or reverse so that no one can understand it other than those who know the order.
    - **Grille ciphers:** A technique used to encrypt plaintext by writing it onto a sheet of paper through a pierced (or stenciled) sheet of paper or cardboard or any other

similar material. In this technique, one can decipher a message using an identical grille. This system is thus difficult to crack and decipher, as only someone with the correct grille would be able to decipher the hidden message.



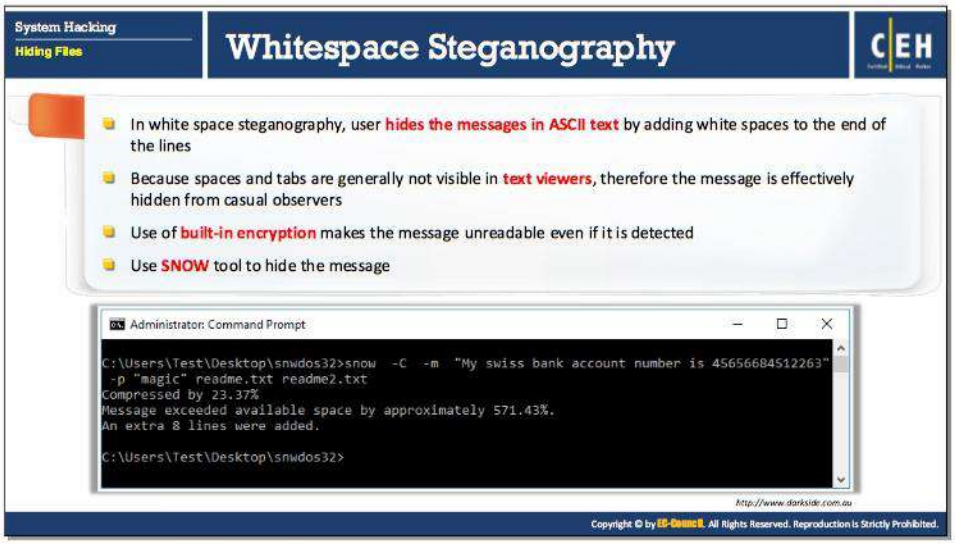
Types of Steganography based on Cover Medium

Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the existence of the message. The increasing uses of electronic file formats with new technologies have made data hiding possible. Basic steganography can be broken down into two areas: data hiding and document making. Document making deals with protection against removal. It's further classification of cover medium includes watermarking and fingerprinting.

The different types of steganography are as follows:

- **Image Steganography:** Images are the popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, .JPG, .BMP, etc.
- **Document steganography:** In the Document steganography, the user adds white spaces and tabs at the end of the lines.
- **Folder Steganography:** Folder Steganography refers to hiding one or more files in a folder. In this process, the user moves the file physically but still keeps associated to its original folder for recovery.
- **Video Steganography:** Video steganography is a technique to hide any kind of files with any extension into a carrying Video file. One can apply video steganography to different formats of files such as .AVI, .MPG4, .WMV, etc.
- **Audio Steganography:** In audio steganography, the user embeds the hidden messages in digital sound format.

- **Whitespace Steganography:** In white space steganography, the user hides the messages in ASCII text by adding white spaces to the end of the lines.
- **Web Steganography:** In web steganography, a user hides web objects behind another objects and uploads them to a webserver.
- **Spam/Email Steganography:** One can use spam emails for secret communication by embedding the secret messages in some way and hiding the embedded data in the spam emails. This technique refers to Spam/Email steganography.
- **DVD-ROM Steganography:** In the DVD-ROM steganography, the user embeds the content in audio and graphical data.
- **Natural Text Steganography:** Natural text steganography is converting sensitive information into a user-definable free speech such as a play.
- **Hidden OS Steganography:** Hidden OS Steganography is the process of hiding one operation system into other.
- **C++ Source Code Steganography:** In the C++ source code steganography, user hides the set of tools in the files.



Whitespace Steganography

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected.

- **Snow**

  Source: *http://www.darkside.com.au*

  Snow is a program for concealing messages in text files by appending tabs and spaces to the end of lines, and for extracting messages from files containing hidden messages. Tabs and spaces are invisible to most text viewers, hence the steganographic nature of this encoding scheme. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs. This usually allows three bits to be stored every eight columns. There is an alternative encoding scheme, using alternating spaces and tabs to represent zeros and ones, but users rejected it because it uses fewer bytes but requires more columns per bit (4.5 vs. 2.67). An appended tab character is an indication of the start of the data, which allows the insertion of mail and news headers without corrupting the data.

  Synopsis: **snow [-CQS] [-p passwd] [-l line-len] [-f file | -m message] [infile [outfile]]**

  Options:

  - **-C**: Compress the data if concealing, or uncompress it if extracting.
  - **-Q**: Quiet mode. If not set, the program reports statistics such as compression percentages and amount of available storage space used.

- **-S**: Report on the approximate amount of space available for hidden message in the text file. Line length is valid, but ignore other options.
- **-p password**: If this is set, the data encryption occurs with this password during concealment, or decrypted during extraction.
- **-l line-length**: When appending whitespace, snow will always produce lines shorter than this value. By default, the line length is 80.
- **-f message-file**: The input text file will hide the contents of this file.
- **-m message-string**: The input text file will hide the contents of this string. Note that, unless a newline is somehow included in the string, it will not appear in the extracted message.

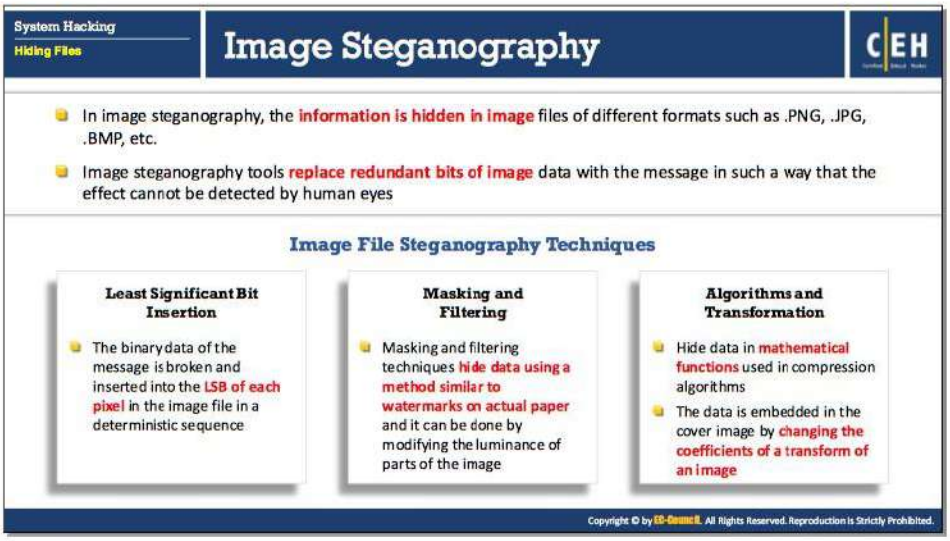


Image Steganography

Image steganography allows you to conceal your secret message within an image. You can take advantage of the redundant bit of the image to conceal your message within it. These redundant bits are those bits of the image that have very little effect on the image, if altered. Detection of this alteration is not easy. You can conceal your information within images of different formats (e.g., .PNG, .JPG, .BMP).

Images are popular "cover objects" used for steganography by replacing redundant bits of image data with the message, in such a way that human eyes cannot detect the effect. Image steganography is classified into two types: image domain and transform domain. In ***image domain*** (spatial) techniques, a user embeds the messages directly in the intensity of the pixels. In ***transformdomain*** (frequency) techniques, first, the transformation of images occurs; then the user embeds the message in the image.

The figure below depicts image steganography process and the role of steganography tools in the process.

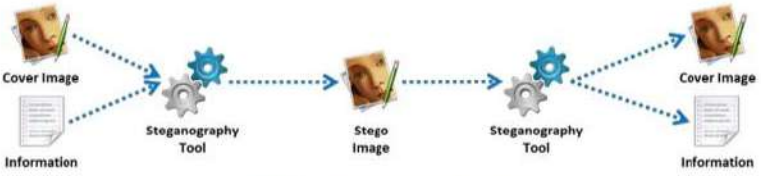


FIGURE 6.4: Image steganography process

Image File Steganography Techniques

- **Least Significant Bit Insertion**

  The least-significant-bit Insertion technique is the most commonly used technique of image steganography, in which the least significant bit (LSB) of each pixel helps hold secret data. The LSB is the rightmost bit of each pixel of an image.

  In least significant bit insertion method, the binary data of the message is broken and inserted into the LSB of each pixel in the image file in a deterministic sequence. Modifying the LSB does not result in a noticeable difference because the net change is minimal and can be indiscernible to the human eye. If changed, the LSB has very little effect on the image; thus, its detection is difficult. To hide the message, first "break" it, then insert each bit in place of each pixel's LSB, so that the recipient can retrieve your message easily.

  Hiding the data:

  - The stego tool makes a copy of an image palette with the help of the red, green, and blue (RGB) model
  - Each pixel of the 8-bit binary number LSB is substituted with one bit of hidden message
  - A new RGB color in the copied palette is produced
  - With the new RGB color, the pixel is changed to 8-bit binary number

  Suppose you have chosen a 24-bit image to hide your secret data, which you can represent in digital form, as follows:

  ```
  (00100111 11101001 11001000) (00100111 11001000 11101001) (11001000
  00100111 11101001)
  ```

  And you want to hide the letter "H" in above 24-bit image. Now system represents letter "H" by binary digits 01001000. To hide this "H," you can change the previous stream as:

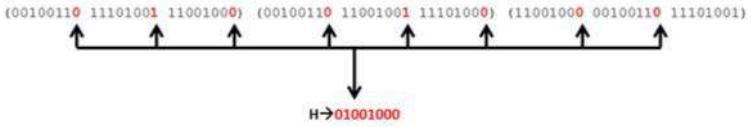
  

  FIGURE 6.5: Example of Least Significant Bit Insertion

  You just need to replace the LSB of each pixel of the image file as shown in this figure. To retrieve this H at the other side, the recipient combines all the LSB image bits and is thus able to detect the H.

- **Masking and Filtering**

  Masking and filtering techniques take advantage of human vision, which cannot detect slight changes in particular images. Grayscale images and digital watermarks can hide information in a way similar to watermarks on paper.

Masking allows you to conceal your secret data by placing it in an image file. You can use masking and filtering techniques on 24-bit-per-pixel and grayscale images. To hide secret messages, you need to adjust the luminosity and opacity of the image. If the change in luminance is small, then people other than intended recipients fail to notice that the image contains a hidden message. You can easily apply this technique to an image, as the image itself remains undisturbed. In most cases, users perform masking of JPEG images. Lossy JPEG images are relatively immune to cropping and compression image operations. Hence, you can hide this information in lossy JPEG images, often using the masking technique. If a message hides in significant areas of the picture, the steganography image encoded with a marking, degrades at a lower rate under JPEG compression.

Masking techniques can be detected with simple statistical analysis but is resistant to lossy compression and image cropping. The information is not hidden in the noise but in the significant areas of the image.

- **Algorithms and Transformation**

  The algorithms and transformation technique is based on hiding the secret information during image compression. In this technique, the user conceals the information by applying various compression algorithms and transformation functions. A compression algorithm and transformation uses a mathematical function to hide the coefficient of the least bit during image compression. The data is embedded in the cover image by changing the coefficients of a transform of an image. Generally, JPEG images are suitable to use for compression, as they can function at different compression levels. This technique provides a high level of invisibility of secret data. JPEG images use a discrete cosine transform to achieve compression.

  There are three types of transformation used in the compression algorithm:

  - Fast Fourier transformation
  - Discrete cosine transformation
  - Wavelet transformation

  If the user embeds the information in the spatial domain that is the LSB insertion technique, information hidden in the images can be vulnerable to attacks. An attacker can make use simple signal processing techniques and damage the information hidden in the image when using the LSB insertion technique. It may refer to loss of compression where the image undergoes some processing techniques like compression. To overcome these problems, one can hide the information with frequency domain–based techniques such as Fast Fourier transformation, discrete cosine transformation, or Wavelet transformation. In the frequency domain, digital data are not continuous. To analyze the data of the image to which frequency domain transformations are applied becomes very difficult, thus avoiding many cryptanalysis attacks on the hidden information.

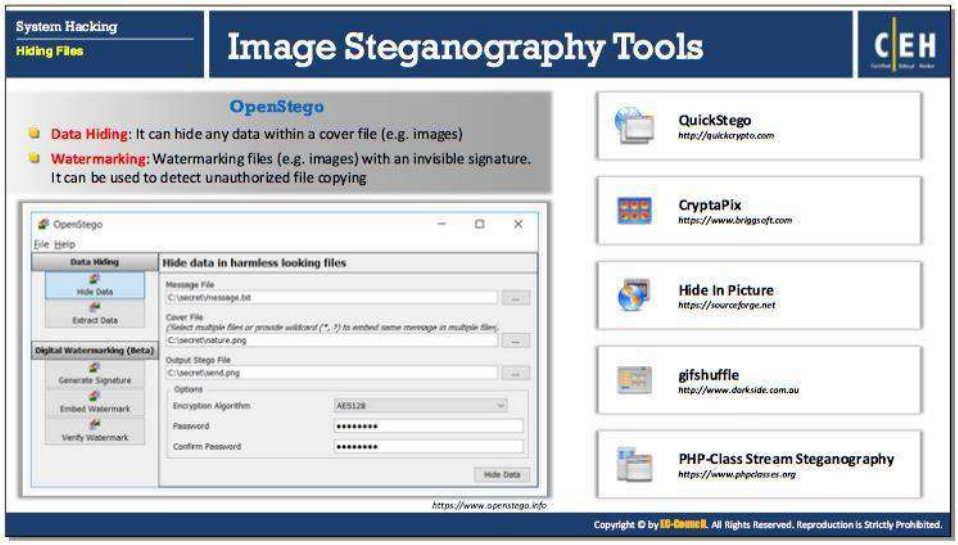


Image Steganography Tools

Image steganography tools detect the hidden content in images where you can insert the hidden data into the redundant bits of data sources. You can use image files such as JPEG, GIF, BMP, and PNG to conceal the data.

- **OpenStego**

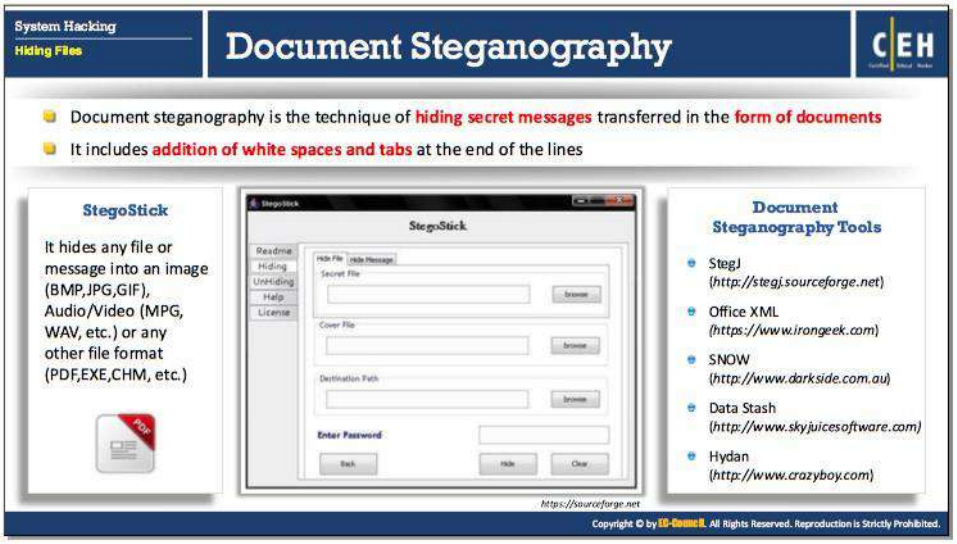
  Source: *https://www.openstego.info*

  OpenStego is a steganography application that provides following functions.

  - **Data Hiding:** It can hide any data within a cover file (e.g. images)
  - **Watermarking:** Watermarking files (e.g. images) with an invisible signature. It can be used to detect unauthorized file copying.

Listed below are some of the image steganography tools:

- QuickStego (*http://quickcrypto.com*)
- CryptaPix (*https://www.briggsoft.com*)
- Hide In Picture (*https://sourceforge.net*)
- gifshuffle (*http://www.darkside.com.au*)
- PHP-Class Stream Steganography (*https://www.phpclasses.org*)
- Steganography Studio (*http://stegstudio.sourceforge.net*)
- OpenPuff (*http://embeddedsw.net*)
- Virtual Steganographic Laboratory (VSL) (*http://vsl.sourceforge.net*)
- Red JPEG XT (*http://www.totalcmd.net*)
- ImageHide (*http://www.dancemammal.com*)



Document Steganography

As with image steganography, ***document*** steganography is the technique of hiding secret messages transferred in the form of documents. It includes addition of whitespaces and tabs at the end of the lines. Stego-document is a cover document comprising of the hidden message. Steganography algorithms, referred to as the "**stego system**, are employed for hiding the secret messages in the cover medium at the sender end. The same algorithm is used for extracting the hidden message from the stego-document by the recipient.

The diagram given below illustrates the document steganography process:

FIGURE 6.6: Document steganography process

Document Steganography Tools

Document steganography tools helps in hiding any file within documents, such as text or html files, using the steganography methods.

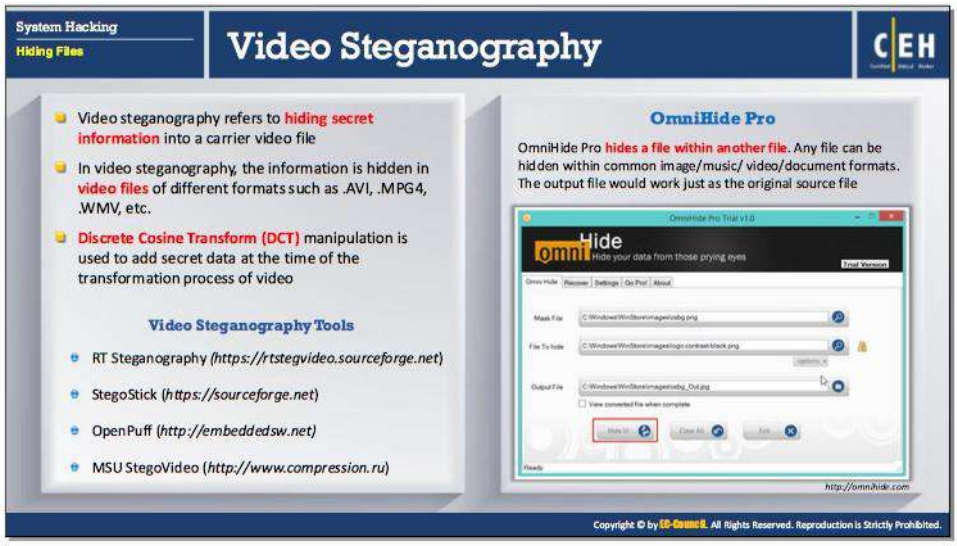
- **StegoStick**

  Source: *https://sourceforge.net*

  StegoStick is a steganographic Tool that lets you hide any file into any file. It is based on image, audio, or video steganography that hides any file or message into an image (BMP, JPG, GIF, etc.), Audio/Video (MPG, WAV, etc.) or any other file format (PDF, EXE, CHM, etc.).

Some of the document steganography tools are listed below:

- StegJ (*http://stegj.sourceforge.net*)
- Office XML (*https://www.irongeek.com*)
- SNOW (*http://www.darkside.com.au*)
- Data Stash (*http://www.skyjuicesoftware.com*)
- Hydan (*http://www.crazyboy.com*)
- Texto (*http://www.eberl.net*)



Video Steganography

The image steganography discussed earlier can only hide a small amount of data inside image carrier files. Thus image steganography can only be used when small amounts of data are to be hidden in the image files. However, one can use video steganography when there is a need to hide large amounts of data inside carrier files.

Video steganography refers to hiding secret information into a carrier video file. The information is hidden in video files of different formats such as .AVI, .MPG4, .WMV, etc. Discrete Cosine Transform (DCT) manipulation is used to add secret data at the time of the transformation process of the video.

Video files here act as the carrier to carry the secret information from one end to another end. It keeps your secret information more secure. A large number of secret messages can be hidden in video files as every frame consists of images and sound. As the carrier video file is a moving stream of images and sound, it is difficult for the unintended recipient to notice the distortion in the video file caused due to the secret message. It might go unobserved because of the continuous flow of the video. You can apply all the techniques available for image and audio steganography to video steganography.

The information hidden in video files is nearly impossible to recognize by the human eye, as the change of a pixel color is negligible. This lessens the probability for the attacker to discover the hidden information from the running video file.

Video Steganography Tools

The following tools act as video steganography utilities for hiding secret information in running video.

- **OmniHide Pro**

  Source: *http://omnihide.com*

  OmniHide PRO allows you to hide any secret file within an innocuous image, video, music files, etc. The user can use or share the resultant Stego file like a normal file without anyone knowing the hidden content, thus this tool enables you to save your secret file from prying eyes. It also enables you to add a password to hide your file to enhance security.

  Features:

  - This allows you to hide your files in Photos, Movies, Documents, and Music etc.
  - It puts no limitation on file type and size you want to hide

Listed below are some of the video steganography tools:

- RT Steganography (*https://rtstegvideo.sourceforge.net*)
- StegoStick (*https://sourceforge.net*)
- OpenPuff (*http://embeddedsw.net*)
- MSU StegoVideo (*http://www.compression.ru*)

Audio Steganography

Audio steganography allows you to conceal your secret message within an audio file such as WAV, AU, and even MP3 audio files. It embeds secret messages in audio files by slightly changing the binary sequence of the audio file. Changes in the audio file after insertion are not easily detectable, so this secures the secret message from prying ears.

You should not allow distortion of the carrier audio file to avoid detection of the hidden messages. Therefore, embed the secret data in such a way that a slight change in the audio file can go unnoticed upon listening. You can hide information in an audio file by replacing the LSB or by using frequencies that are not audible to the human ear (>20,000 Hz).

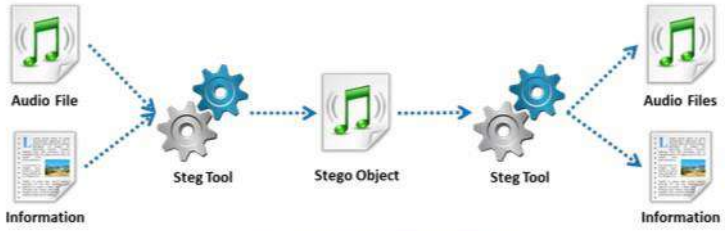


FIGURE 6.7: Audio steganography process

Audio Steganography Methods

There are certain methods available to conceal your secret messages in audio files. Some methods implement the algorithm that relies on inserting the secret information in the form of a noise signal, while other methods believe in exploiting sophisticated signal processing techniques to hide information.

The following methods help to perform audio steganography in order to hide information:

- **Echo Data Hiding**

  In the echo data hiding method, you can embed the secret information in the carrier audio signal by introducing an echo into it. It uses three parameters of echo, namely, initial amplitude, decay rate, and offset or delay to hide secret data. When the offset between carrier signal and echo decreases, they combine at a certain point of time where it is not possible for the human ear to distinguish between these two signals. At this point, you can hear an echo sound as an added resonance to the original signal. However, this point of indistinguishable sounds depends on factors such as quality of original audio signal, type of sound, and listener acuity.

  To encode the resultant signal into binary form, two different delay times are used. These delay times should be below human perception. Parameters such as decay rate and initial amplitude should also be set below threshold audible values so that the audio cannot be heard.

- **Spread Spectrum Method**

  This method uses two versions of spread spectrum, direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS).

  - **Direct Sequence Spread Spectrum (DSSS):** DSSS is a frequency modulation technique where a communication device spreads a signal of low bandwidth over a broad frequency range to enable sharing of a single channel among multiple users. The DSSS steganography technique transposes the secret messages in the radio wave frequencies. DSSS does introduce some random noise to the signal.
  - **Frequency Hopping Spread Spectrum (FHSS):** In FHSS, the user alters the audio file's frequency spectrum so that it hops rapidly between frequencies. Spread spectrum method plays a major role in secure communications, both commercial and military.

- **LSB Coding**

  LSB encoding works similarly to the LSB insertion technique in which users can insert a secret binary message in the least significant bit of each sampling point of the audio signal. This method allows one to hide large amounts of secret data. It is possible to use the last two significant bits to insert secret binary data, but at the risk of creating noise in the audio file. Its poor immunity to manipulation makes this method less adaptive. You can easily identify extra hidden data because of channel noise and resampling.

- **Tone Insertion**

  This method involves embedding data in the audio signal by inserting low power tones. These low power tones are not audible in the presence of significantly higher audio signals. As it is not audible, it conceals the existence of your secret message. It is very difficult for an eavesdropper to detect the secret message from the audio signal. This method helps to avoid attacks such as low-pass filtering and bit truncation. The audio

steganography software implements one of these audio steganography methods to embed the secret data in the audio files.

- **Phase Encoding**

  Phase coding is described as the phase in which an initial audio segment is substituted by a reference phase that represents the data. It encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving a soft encoding in terms of signal-to-noise ratio.

Audio Steganography Tools

There are many tools available in the market, which can help you to hide your secret information in the audio file. The following are some of the audio steganography tools to hide your secret information in audio files:

- **DeepSound**

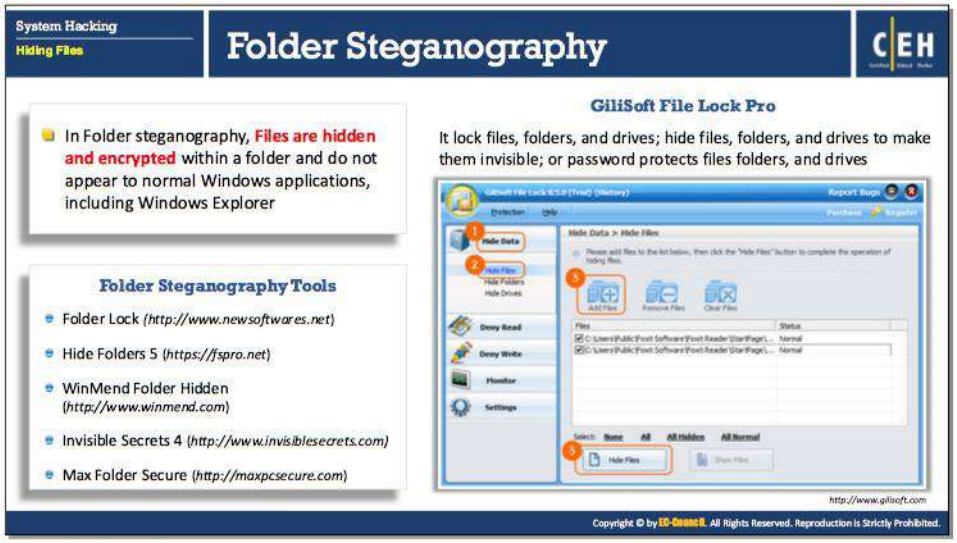
  Source: *http://jpinsoft.net*

  DeepSound allows you to hide any kind of secret data in audio files (WAV and FLAC). You can use this tool to embed your secret message in the audio file. It will also allow you to extract secret files directly from audio CD tracks when you are at the other end. In addition, it is able to encrypt secret files, thus enhancing security.

  To access the data in a carrier file, you simply browse to the location with the DeepSound file browser and right-click the audio file to extract your secret file(s).

Some of the audio steganography tools are listed below:

- BitCrypt (*http://bitcrypt.moshe-szweizer.com*)
- SilentEye (*http://silenteye.v1kings.io*)
- CHAOS Universal (*http://safechaos.com*)
- StegoStick (*https://sourceforge.net*)
- MP3Stego (*http://www.petitcolas.net*)
- Hide4PGP (*http://www.heinz-repp.onlinehome.de*)
- MAXA Security Tools (*http://www.maxa-tools.com*)
- QuickCrypto (*http://www.quickcrypto.com*)



Folder Steganography

Folder steganography refers to hiding secret information in folders. Files are hidden and encrypted within a folder and are not seen by the normal Windows applications, including Windows Explorer.

Folder Steganography Tools

Folder steganography tools help to secure the folders and protect the data. These tools secure using different encryption techniques. It can hide the folders, which contain the confidential data.

- **GiliSoft File Lock Pro**

  Source: *http://www.gilisoft.com*

  GiliSoft File Lock Pro restricts access to files, folders and drivers, lock files, folders and drives, hides files, folders and drives to make them invisible, or password protects files folders and drives. You can use this utility to password protect or hide files, folders and drives. With this program, nobody can access or destroy your private data without a password.

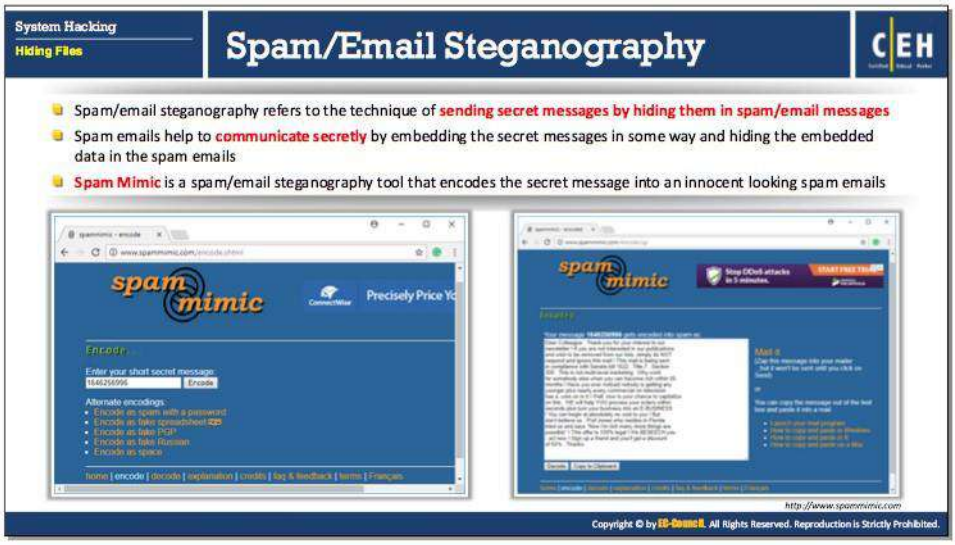
  Features:

  - Hide your private files/folders from a local disk or external (USB) disk, completely invisible to anyone or any programs even under Windows Safe Mode.
  - Password protect any type files/folders on local disk or external (USB) disk, password protect a folder so all new files added become password protected also.

- After protecting the files/folders on local disk, people can read the write-protected files, but nobody can modify, delete (even shift delete), or rename it without a password.
- Monitor a disk or a folder and its sub-folders when changing and writing or any operations or changes made by a user.
- Encrypt files and folders into GFL format or EXE format file with AES encryption algorithm.

Some of the folder steganography tools are listed below:

- Folder Lock (*http://www.newsoftwares.net*)
- Hide Folders 5 (*https://fspro.net*)
- WinMend Folder Hidden (*http://www.winmend.com*)
- Invisible Secrets 4 (*http://www.invisiblesecrets.com*)
- Max Folder Secure (*http://maxpcsecure.com*)
- QuickCrypto (*http://www.quickcrypto.com*)
- Universal Shield (*http://www.everstrike.com*)



Spam/Email Steganography

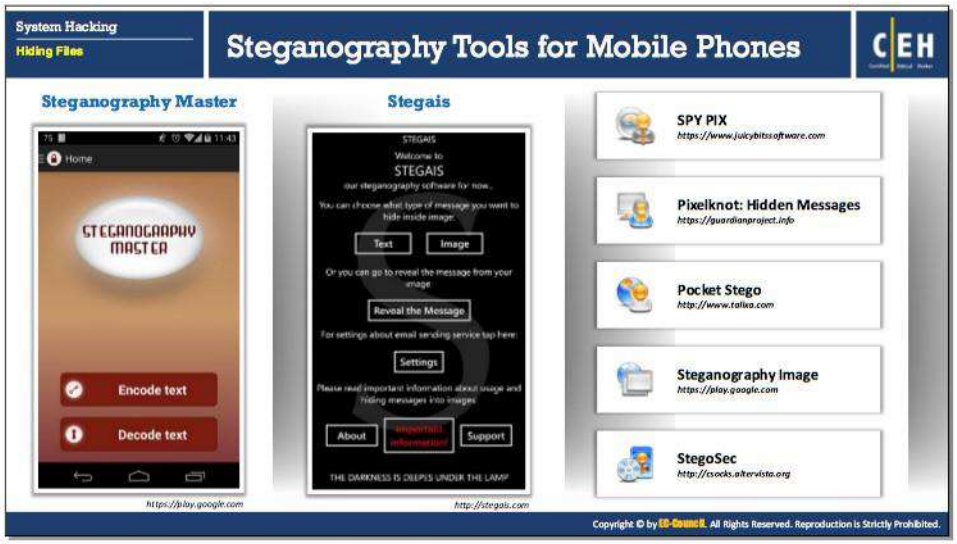
Spam/email steganography refers to the technique of sending secret messages by hiding them in spam/email messages. Spam emails help to communicate secretly by embedding the secret messages in some way and hiding the embedded data in the spam emails. Various military agencies supposedly use this technique with the help of steganography algorithms. You can use Spam Mimic tool to hide the secret message in the mail.

Spam/Email Steganography Tool

- **Spam Mimic**

  Source: *http://www.spammimic.com*

  Spam Mimic is spam "grammar" for a mimic engine by Peter Wayner. This encodes the secret message into innocent looking spam emails. The fun grammar of this software encodes the message into art-speak and the commentary of a baseball game. It provides the capabilities of both encoding and decoding. The encoder of this tool encodes the secret message as spam with a password, fake PGP, fake Russian, and space.



Steganography Tools for Mobile Phones

Earlier, we discussed a wide range of applications/tools that can be useful in hiding secret messages in various types of carrier media such as images, audio, video, and text. These tools run on a variety of platforms of desktops or laptops only. However, there are also many mobile apps available that act as steganography tools for mobile phones. Mobile users can use these apps to send their secret messages. Below are some of the steganography tools that run on mobile devices:

- **Steganography Master**

  Source: *https://play.google.com*

  Steganography Master helps in hiding a secret message inside a photo. You can encode a message in a picture, then save it or send it to any mobile users. You can decode the message only with the same app, but if you want to ensure that only the intended receiver can read the message, you can also provide a password.

- **Stegais**

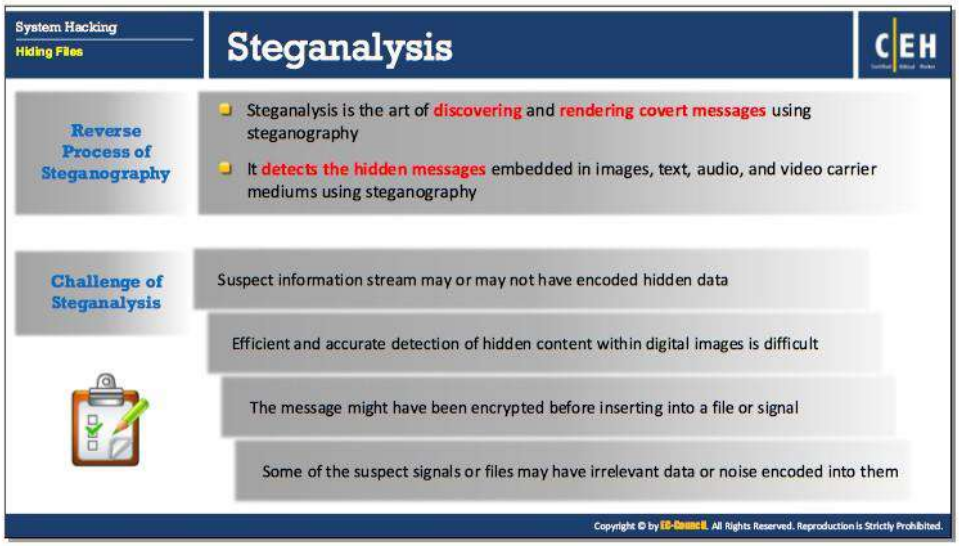
  Source: *http://stegais.com*

  Stegais can:

  - Hide the message in a selected image from the photo library or in a taken photo from the camera
  - Send an image which contains a hidden message to another person through email or just save it to the photo library
  - Reveal the hidden message from the image

Below is the list of some additional steganography tools for mobile phones:

- SPY PIX (*https://www.juicybitssoftware.com*)
- Pixelknot: Hidden Messages (*https://guardianproject.info*)
- Pocket Stego (*http://www.talixa.com*)
- Steganography Image (*https://play.google.com*)
- StegoSec (*http://csocks.altervista.org*)
- StegDroid Alpha (*https://play.google.com*)
- Da Vinci Secret Image (*https://play.google.com*)
- Steg-O-Matic (*https://itunes.apple.com*)
- Secret Tidings (*https://play.google.com*)
- Steganography (*https://github.com*)
- Steganography Application (*https://play.google.com*)



Steganalysis

Steganalysis is the process of discovering the existence of the hidden information in a medium. Steganalysis is the reverse process of steganography. It is one of the attacks on information security in which attacker called a steganalyst tries to detect the hidden messages embedded in images, text, audio and video carrier mediums using steganography. Steganalysis determines the encoded hidden message, and if possible, it recovers that message. It can detect the message by looking at variances between bit patterns and unusually large file sizes.

Steganalysis contains two aspects: the ***detection*** and ***distortion*** of messages. In the detection phase, the analyst observes the relationships between the steganography tools, stego-media, cover and message. In the distortion phase, the analyst manipulates the stego-media to extract the embedded message and decides whether it is useless and should be removed altogether.

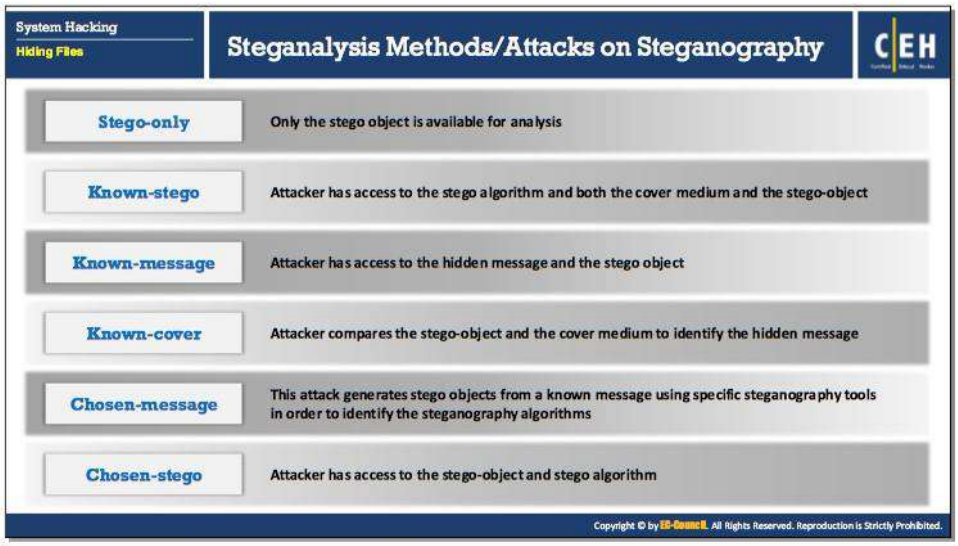
The first step in steganalysis is to discover a suspicious image that may be harboring a message. This is an attack on the hidden information. There are two other types of attack against steganography: ***message*** and ***chosen-message*** attacks. In the former, the steganalyst has a known hidden message in the corresponding stego-image. The steganalyst determines patterns that arise from hiding the message and detecting this message. The steganalyst creates a message using a known stego tool and analyzes the differences in patterns. In a chosen-message attack, the attacker creates steganography media using the known message and steganography tool (or algorithm).

Cover images disclose more visual clues than do stego-images. It is necessary to analyze the stego-images to identify the concealed information. The gap between the cover image and the stego-image file size is the simplest signature. Many signatures are evident using some of the color schemes of the cover image.

Once detected, an attacker can destroy a stego-image or modify the hidden messages. It is very important to understand the overall structure of the technology and methods to detect the hidden information for uncovering the activities.

Some of the challenges of stegoanalysis are given below:

- Suspect information stream may or may not have encoded hidden data.
- Efficient and accurate detection of hidden content within digital images is difficult.
- The message might have been encrypted before being inserted into a file or signal.
- Some of the suspect signals or files may have irrelevant data or noise encoded into them.



Steganalysis Methods/Attacks on Steganography

Steganography attacks work according to what type of information is available for the steganalyst to perform steganalysis. This information may include hidden message, carrier (cover) medium, stego object, steganography tools or algorithms used for hiding information. Thus, the classification of steganalysis includes six types of attacks: stego-only, known-stego, known-message, known-cover, chosen-message, and chosen-stego.

- **Stego-only attack**

  In stego-only attack, the steganalyst or the attacker does not have access to any information except the stego-medium or stego object. In this attack, the staganalyst needs to try every possible steganography algorithm and related attack to recover the hidden information.

- **Known-stego attack**

  This attack allows attacker to know the steganography algorithm as well as original and stego-object. The attacker can extract the hidden information with the information at hand.

- **Known-message attack**

  The known-message attack presumes that the message and the stego-medium are available. Using this attack, one can detect the technique used to hide the message.

- **Known-cover attack**

  Attackers use the known-cover attack when they have knowledge of both the stego-object and the original cover-medium. This will enable a comparison between both the

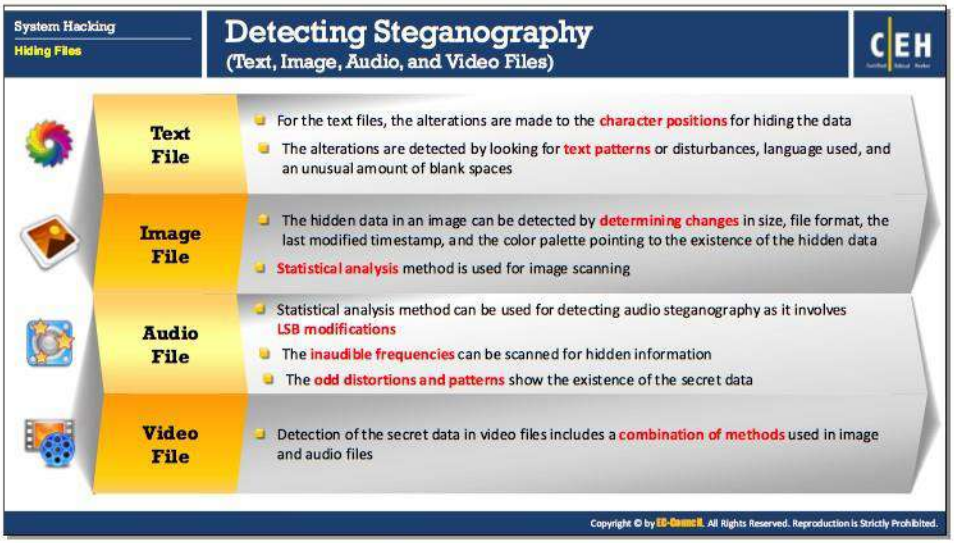
mediums in order to detect the changes in the format of the medium and find the hidden message.

- **Chosen-message attack**

  The steganalyst uses known message to generate a stego-object by using some steganography tool in order to find the steganography algorithm used for hiding the information. The goal in this attack is to determine patterns in the stego-object that may point to the use of specific steganography tools or algorithms.

- **Chosen-stego attack**

  The chosen-stego attack takes place when the steganalyst knows both a stego object and steganography tool or algorithm used to hide the message.



Detecting Steganography (Text, Image, Audio and Video Files)

Steganography is the art of hiding either confidential or sensitive information within the cover medium. In this, the unused bits of data in computer files such as graphics, digital images, text, HTML, etc. help in hiding sensitive information from unauthorized users. Detection of hidden data includes different ways depending on the file used.

The following file types require specific methods to detect hidden messages.

- **Text Files**

  For the text files, the alterations are made to the character positions for hiding the data. One can detect these alterations by looking for text patterns or disturbances, the language used, line height, and unusual number of blank spaces. A simple word processor can reveal the text steganography sometimes as it displays the spaces, tabs, and other characters that distort the text's presentation during text steganography.

  By taking a closer look at the following things, you can detect text steganography:

  - Unusual patterns used in stego object
  - Appended extra spaces and invisible characters

- **Image Files**

  The information that is hidden in the image can be detected by determining changes in size, file format, last modified, last modified time stamp, and color palette of the file.

  The following points can help you to detect image steganography:

  - Too many display distortions in images

- Sometimes images may become grossly degraded
- Detection of anomalies through evaluating too many original images and stego images with respect to color composition, luminance, pixel relationships, etc.
- Exaggerated "noise"

Statistical analysis methods help to scan an image for steganography. Whenever you insert a secret message into an image, LSBs are no longer random. With encrypted data that has high entropy, the LSB of the cover will not contain the information about the original and is more or less random. By using statistical analysis on the LSB, you can identify the difference between random values and real values.

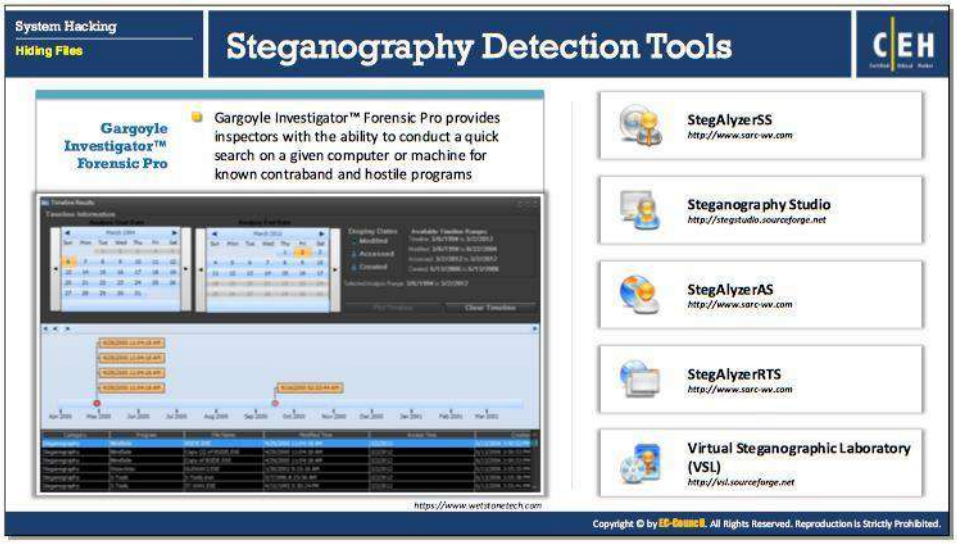
- **Audio Files**

  Audio steganography is a process of embedding confidential information such as private documents and files in digital sound. Statistical analysis methods can be used for detecting audio steganography as it involves LSB modifications. The inaudible frequencies can be scanned for hidden information. The odd distortions and patterns show the existence of the secret data

- **Video Files**

  Detection of the secret data in video files includes a combination of methods used in image and audio files. Special code signs and gestures help in detecting secret data.

Both audio and video steganography is quite difficult to detect, as compared to other types such as image, and document. Moreover, it is very hard to detect good steganography of any type. However, careful analysis of audio and video signals for hidden information may create chances of detecting it correctly.



Steganography Detection Tools

Steganography detection tools allow you to detect and recover hidden information in any digital media such as images, audio, and video.

- **Gargoyle Investigator™ Forensic Pro**

  Source: *https://www.wetstonetech.com*

  Gargoyle Investigator™ Forensic Pro is a tool that conducts quick searches on a given computer or machine for known contraband and malicious programs. The tool can find remnants in a removed program as it conducts a search for individual files associated with a particular program. Its signature set contains over 20 categories, including botnets, Trojans, steganography, encryption, and keyloggers, and helps in detecting stego files created by using BlindSide, WeavWav, S-Tools, and others. It has the ability to perform a scan on a stand-alone computer or network resources for known malicious programs, the ability of scan within archive files, and so on.

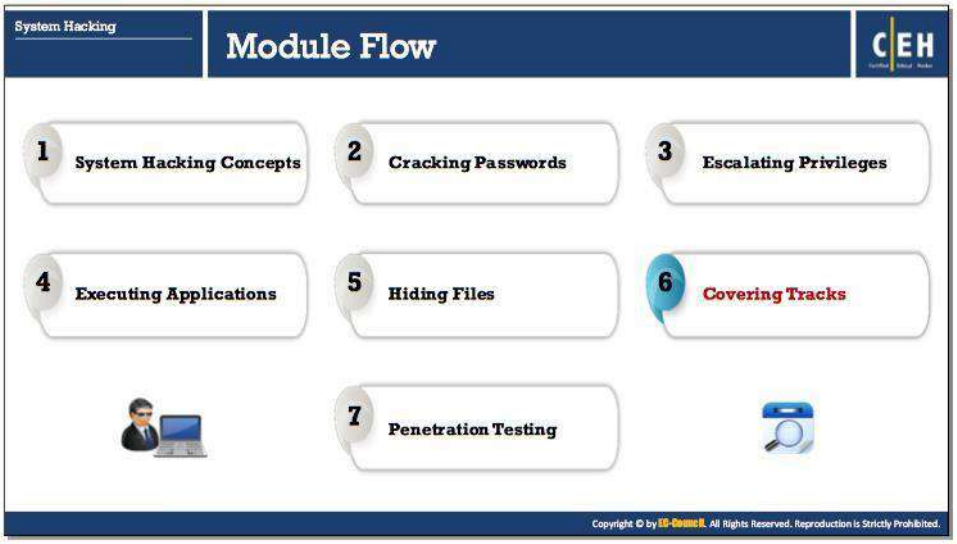
  Features:

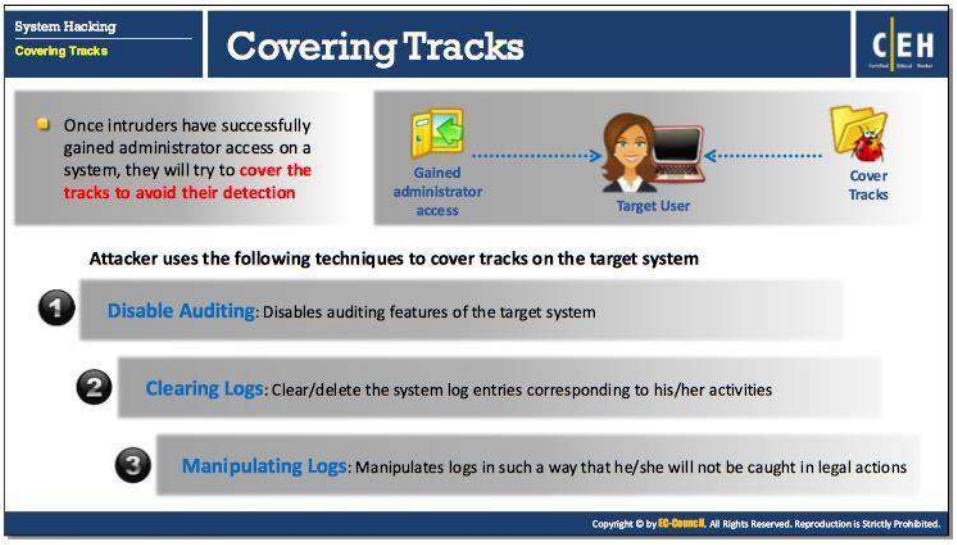
  - The program is capable to scan for known contraband and hostile programs on a stand-alone system or network resource
  - It is interoperable with popular forensic tools such as EnCase™
  - The program provides detailed forensic evidence reports with secure source time stamping, XML based, and is customizable

Some of the steganography detection tools are listed below:

- StegAlyzerSS (*http://www.sarc-wv.com*)

- Steganography Studio (*http://stegstudio.sourceforge.net*)
- StegAlyzerAS (*http://www.sarc-wv.com*)
- StegAlyzerRTS (*http://www.sarc-wv.com*)
- Virtual Steganographic Laboratory (VSL) (*http://vsl.sourceforge.net*)
- Stegdetect (*https://github.com*)





Covering Tracks

In the previous section, we have seen how an attacker hides malicious files on a target computer using various steganographic techniques, NTFS streams, among others, to maintain future access to the target. Now that the attacker has succeeded in performing this malicious operation, the next step will be to remove any resultant traces/tracks in the system.

Covering tracks is one of the main stage during system hacking. In this stage, the attacker tries to hide and avoid being detected, or "traced out," by covering all "tracks," or logs, generated while gaining access to the target network or computer. Let's see how attacker removes traces of an attack in the target computer.

Erasing evidence is a requirement for any attacker who would like to remain obscure. This is one method to evade a trace back. This starts with erasing the contaminated logs and possible error messages generated in the attack process. Then, attackers make changes in the system configuration so that it does not log future activities. By manipulating and tweaking the event logs, attackers trick the system administrator in believing that there is no malicious activity in the system, and that no intrusion or compromise has actually taken place.

Because the first thing a system administrator does in monitoring unusual activity is to check the system log files, it is common for intruders to use a utility to modify these logs. In some cases, rootkits can disable and discard all existing logs. Attackers remove only those portions of logs that can reveal their presence if they intend to use the system for a longer period as a launch base for the future exploitations.

It is imperative for attackers to make the system appear as it did before access was gained and a backdoor established. This allows them to change any file attributes back to their original state. Information listed, such as file size and date, is just attribute information contained in the file.

Protecting against attackers trying to cover their tracks by changing file information can be difficult. However, it is possible to detect whether an attacker has done so by calculating the file's cryptographic hash. This type of hash is a calculation of the entire file before encryption.

Attackers may not wish to delete an entire log to cover their tracks, as doing so may require admin privileges. If attackers are able to delete only attack event logs, they will still be able to escape detection.

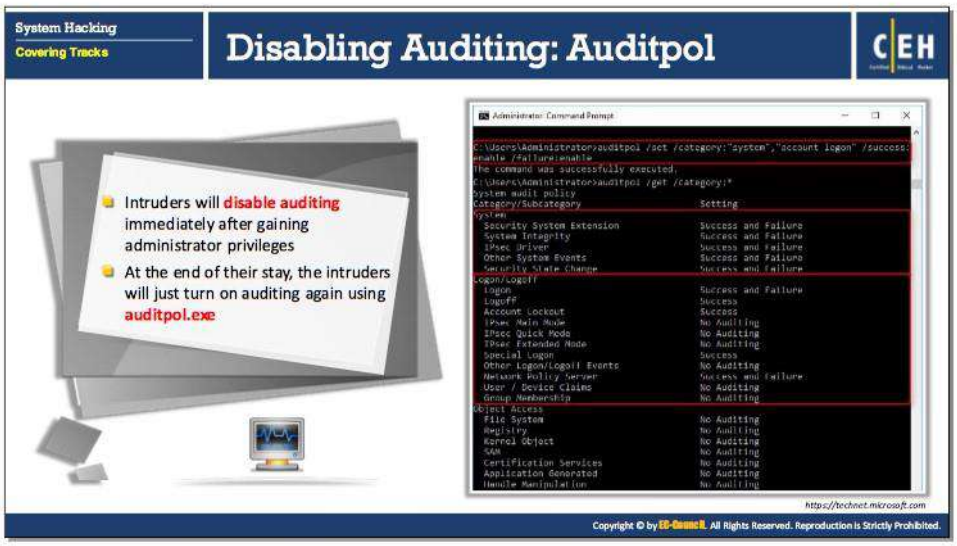
- The attacker can manipulate the log files with the help of: **SECEVENT.EVT** (security): failed logins, accessing files without privileges
- **SYSEVENT.EVT** (system): Driver failure, things not operating correctly
- **APPEVENT.EVT** (applications)

Techniques used for Covering Tracks

The main activities that an attacker performs toward removing his/her traces on the computer are:

- **Disable auditing:** An attacker disables auditing features of the target system
- **Clearing logs:** An attacker clears/deletes the system log entries corresponding to his/her activities
- **Manipulating logs:** An attacker manipulates logs in such a way that he/she will not be caught in legal actions

Thus, the complete job of an attacker involves not only compromising the system successfully, but also disabling logging, clearing log files, eliminating evidence, planting additional tools, and covering his/her tracks.



Disabling Auditing: Auditpol

Source: *https://technet.microsoft.com*

One of the first steps for an attacker who has command-line capability is to determine the auditing status of the target system, locate sensitive files (such as password files), and implant automatic information gathering tools (such as a keystroke logger or network sniffer).

Windows records certain events to the Event Log (or associated syslog). The log can be set to send alerts (email, pager, and so on) to the system administrator. Therefore, the attacker will want to know the auditing status of the system he/she is trying to compromise before proceeding with his/her plans.

Auditpol.exe is the command line utility tool to change Audit Security settings at the category and sub-category levels. Attackers can use AuditPol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

The attacker would establish a null session to the target machine and run the command:

```
C:\>auditpol \\<ip address of target>
```

This will reveal the current audit status of the system. He or she can choose to disable the auditing by:

```
C :\>auditpol \\<ip address of target> /disable
```

This will make changes in the various logs that might register the attacker's actions. He/she can choose to hide the registry keys changed later on.

The moment that intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they again turn on auditing by using the same tool (audit.exe).

Attackers can use AuditPol to view defined auditing settings on the target computer, running the following command at the command prompt:

```
auditpol /get /category:*
```

Clearing Logs

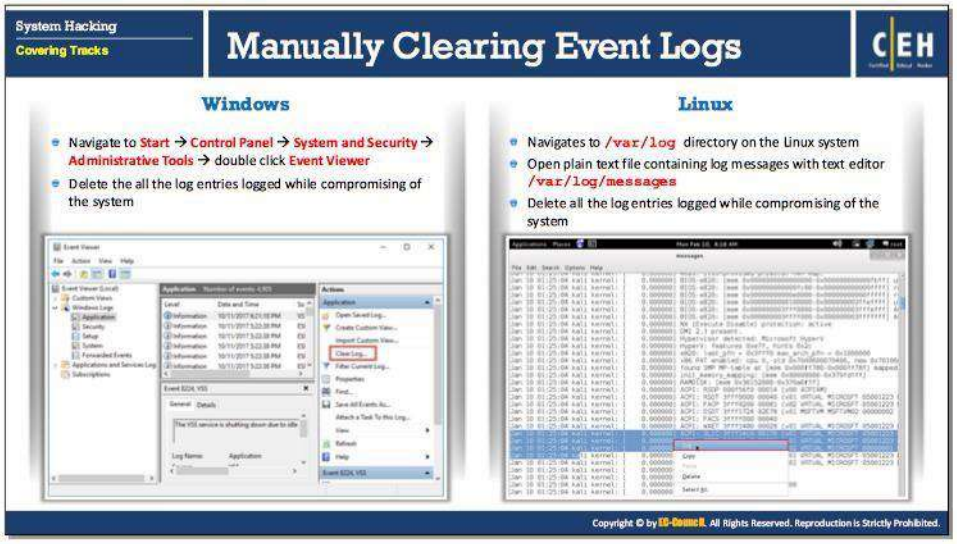
The Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt, PowerShell, and using a BAT file to delete security, system, and application logs on the target system. Attackers might use this utility, wiping out the logs as one method of covering their tracks on the target system.

- **Steps to clear logs using Clear_Event_Viewer_Logs.bat utility**
  1. Download the **Clear_Event_Viewer_Logs.bat** utility from the ***https://www.tenforums.com***
  2. Unblock the .bat file
  3. Right click or press and hold on the .bat file, and click/tap on **Run as administrator**.
  4. If prompted by **UAC**, click/tap on **Yes**.
  5. A command prompt will now open to clear the event logs. The command prompt will automatically close when finished.
- **Steps to clear logs using clearlogs.exe utility**
  1. Download the **clearlogs.exe** utiliy from http://www.ntsecurity.nu
  2. Run clearlogs.exe from the command prompt, and clear the security, system, and application logs using the following options
     - `C:\clearlogs.exe -app`(for clearing application logs)
     - `C:\clearlogs.exe -sec`(for clearing application logs)
     - `C:\clearlogs.exe -sys`(for clearing application logs)

- **Steps to clear logs using meterpreter shell**

  If the system is exploited with the Metasploit, the attacker uses a **meterpreter shell** to wipe out all the logs from a Windows system:

  1. Launch **meterpretershell prompt** of the Metasploit Framework.
  2. Type **`clearev`** command in meterpreter shell prompt and press **Enter**. The logs of the target system will start being wiped out.



Manually Clearing Event Logs

Once attackers gain administrative access to a target system, they can then manually wipe out the log entries corresponding to their activities on both the Windows and the Linux computers. Given below are the steps to clear event logs on Windows and Linux operating systems, respectively.

For Windows

- Navigate to **Start → Control Panel → System and Security → Administrative Tools →** double click **Event Viewer**
- Delete the all the log entries logged while compromising of the system

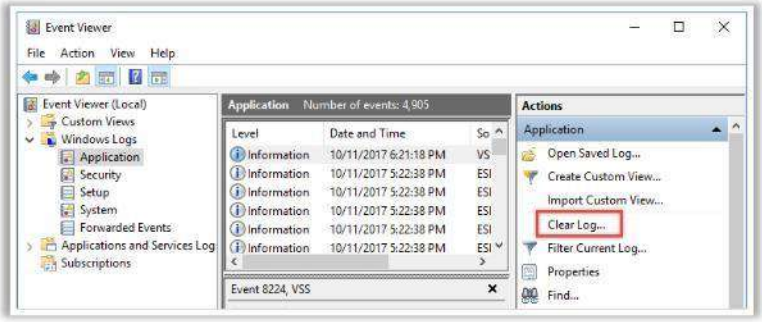


FIGURE 6.8: Clearing Event logs for Windows

For Linux

- Navigates to **/var/log** directory on the Linux system
- Open plain text file containing log messages with text editor **/var/log/messages**
- Delete the all the log entries logged while compromising of the system

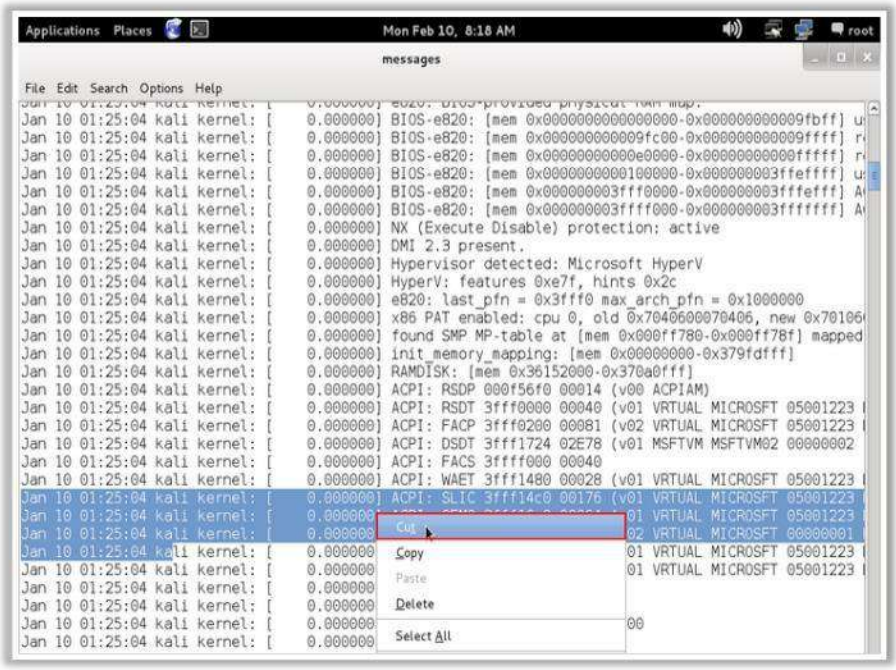
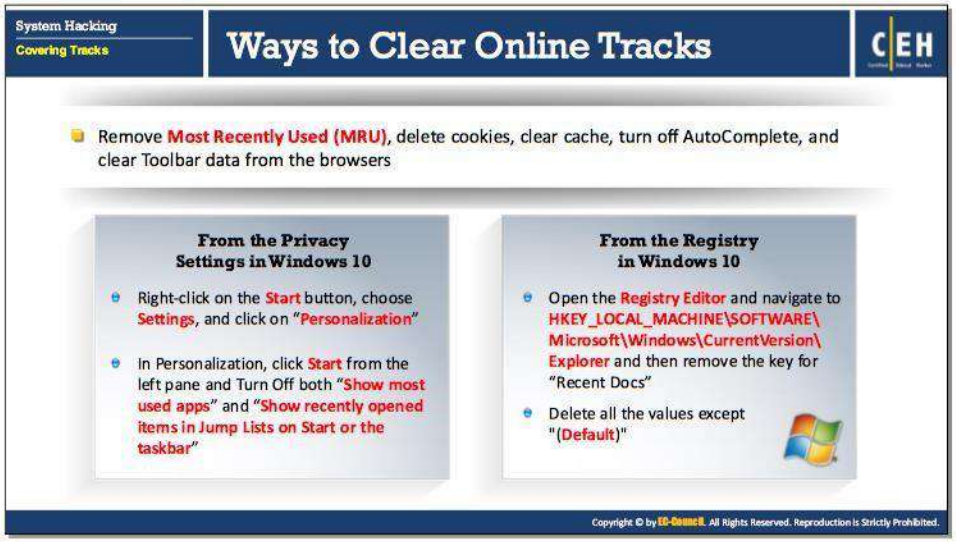


FIGURE 6.9: Clearing Event logs for Linux



Ways to Clear Online Tracks

Attackers clear online tracks maintained using web history, logs, cookies, cache, downloads, visited time, and others on the target computer, so that victims cannot notice what online activities attackers have performed.

What attackers can do to clear their online tracks?

- Use private browsing
- Delete history in the address field
- Disable stored history
- Delete private data
- Clear cookies on exit
- Clear cache on exit
- Delete downloads
- Disable password manager
- Clear data in password manager
- Delete saved sessions
- Delete user JavaScript
- Set up multiple users
- Remove Most Recently Used (MRU)
- Clear Toolbar data from the browsers
- Turn off AutoComplete

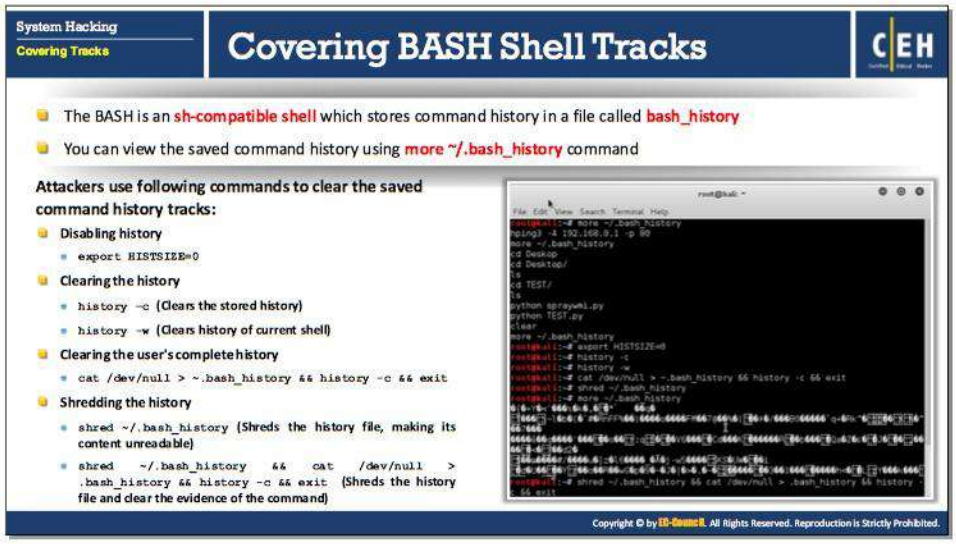
To clear online tracks of various activities, attackers should follow different paths for different operating systems.

Given below are the steps to clear online tracks from the Privacy Settings or from the Windows registry (Windows 10):

- **From the Privacy Settings in Windows 10**
  - Right-click on the **Start** button, choose **Settings**, and click on **Personalization**

- In Personalization, click **Start** from the left pane and Turn Off both **"Show most used apps"** and **"Show recently opened items in Jump Lists on Start or the taskbar"**

- **From the Registry in Windows 10**
  - Open the **Registry Editor** and navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer** and then remove the key for "Recent Docs"
  - Delete all the values except "**(Default)**"



Covering BASH Shell Tracks

The BASH or Bourne Again Shell is a shy-compatible shell which stores command history in a file called bash history. You can view the saved command history using **`more ~/.bash_history`** command.

This feature of BASH is a problem for hackers as the bash_history file could be used by investigators in order to track the origin of an attack and the exact commands used by an intruder in order to compromise a system.

Attackers use following commands to clear the saved command history tracks:

- **Disabling history**

  `export HISTSIZE=0`

  This command disables the BASH shell from saving the history. **HISTSIZE** determines the number of commands to be saved, which will be set to 0 after executing this command. After an execution of this command, an attacker loses a privilege to review the earlier used commands.

- **Clearing the history**
  - **`history -c`**

    This command is useful in clearing the stored history. It is an effective alternate to disabling history command as in this command an attacker has the convenience of rewriting or reviewing the earlier used commands.

- **history -w**

  This command only deletes the history of the current shell whereas the command history of other shells remain unaffected.

- **Clearing the user's complete history**

  cat /dev/null > ~.bash_history&& history -c && exit

  This command deletes the complete command history of the current and all the other shells and exits the shell.

- **Shredding the History**

  - **shred ~/.bash_history**

    This command shreds the history file, making its contents unreadable. It is useful in a case where an investigator locates the file but due to this command, he would be unable to read any command in a history file.

  - **shred ~/.bash_history&& cat /dev/null > .bash_history&& history -c && exit**

    This command firstly, shreds the history file, then deletes it and finally clears the evidence of using this command.

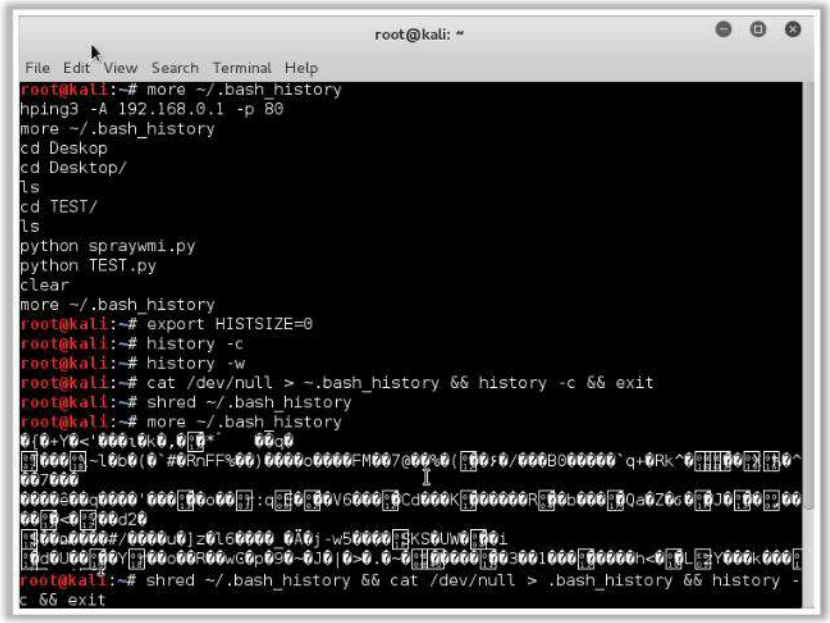
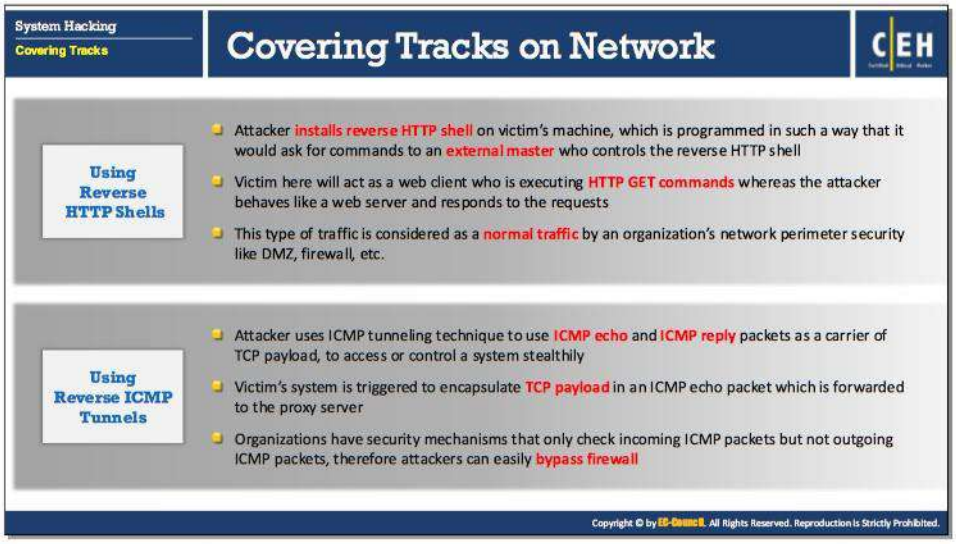
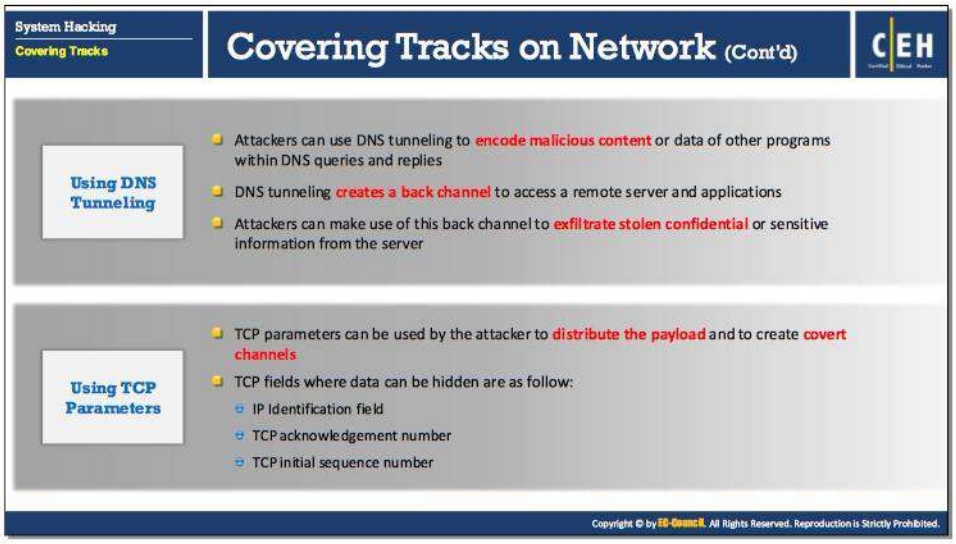


FIGURE 6.10: Covering BASH Shell tracks





Covering Tracks on Network

- **Using Reverse HTTP Shells**

  An attacker starts this attack by first infecting a victim's machine by some malicious code and thereby, installing reverse HTTP shell on the victim's system. This reverse HTTP shell is programmed in such a way that it would ask for commands to an external master

who controls the reverse HTTP shell on a regular basis. This type of traffic is considered as normal traffic by an organization's network perimeter security like DMZ, firewall, etc.

Once an attacker types something on the master system, the command is retrieved and executed on the victim's system. The victim here will act as a web client who is executing HTTP GET commands whereas the attacker behaves like a web server and responds to the requests. Once the previous commands get executed, the results are sent in the next web request.

All the other users in the network can normally access the internet, therefore, this traffic between the attacker and the victim is seen as a normal traffic.

- **Using Reverse ICMP Tunnels**

  ICMP tunneling is a technique where an attacker uses ICMP echo and ICMP reply packets as a carrier of TCP payload, in order to access or control a system stealthily. This method can be used to easily bypass firewall rules because most of the organizations have security mechanisms that only check incoming ICMP packets but not outgoing ICMP packets.

  An attacker first configures the local client to connect with the victim. The victim's system is triggered to encapsulate a TCP payload in an ICMP echo packet which is forwarded to the proxy server. The proxy server de-encapsulates and extracts the TCP payload and sends it to the attacker.

- **Using DNS Tunneling**

  Attackers can use DNS tunneling to encode malicious content or data of other programs within DNS queries and replies. DNS tunneling usually includes data payload that can be added to the victim's DNS server to create a back channel to access a remote server and applications.

  Attackers can make use of this back channel to exfiltrate stolen, confidential or sensitive information from the server.

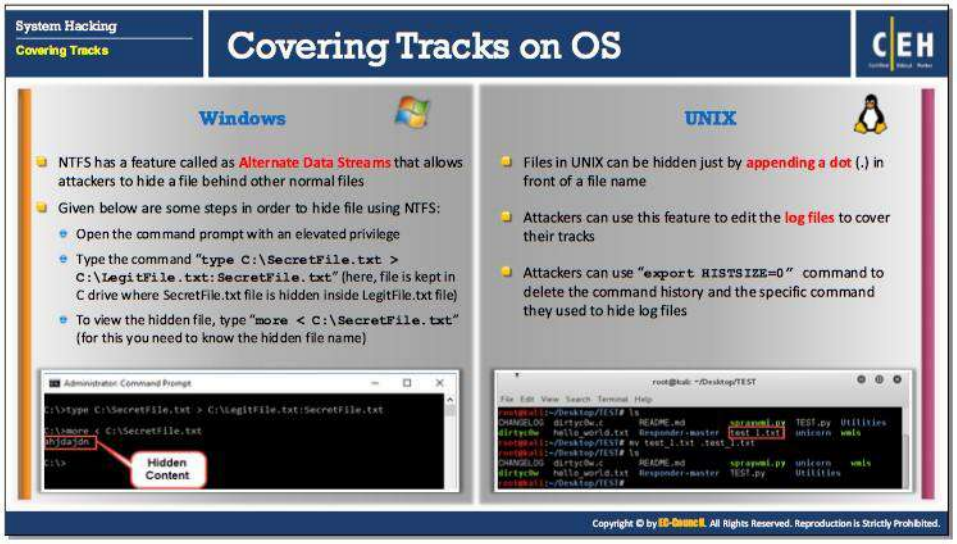
  Attackers perform DNS tunneling in various stages; firstly, they compromise an internal system to have a connection with an external network. Then, they use that compromised system as a command and control server to access the system remotely and transfer files covertly from within the network to outside the network.

- **Using TCP Parameters**

  TCP parameters can be used by the attacker to distribute the payload and to create covert channels. Some of the TCP fields where data can be hidden are as follow:

  - **IP Identification field:** This is an easy approach where a payload is transferred bitwise over an established session between two systems. Here, one character is encapsulated per packet.

- **TCP acknowledgement number:** This approach is quite difficult as it uses a bounce server that receives packets from the victim and sends it to an attacker. Here, one hidden character is relayed by the bounce server per packet.
- **TCP initial sequence number:** This method also does not require an established connection between two systems. Here, one hidden character is encapsulated per SYN request and Reset packets.



Covering Tracks on OS

- **Windows**

  NTFS has a feature called as Alternate Data Streams that allows attackers to hide a file behind other normal files. Given below are some steps in order to hide file using NTFS:

  - Open the command prompt with an elevated privilege
  - Type the command "**`type C:\SecretFile.txt >C:\LegitFile.txt:SecretFile.txt`**" (here, file is kept in C drive where SecretFile.txt file is hidden inside LegitFile.txt file)
  - To view the hidden file, type "**`more < C:\SecretFile.txt`**" (for this you need to know the hidden file name)

- **UNIX**

  Files in UNIX can be hidden just by appending a dot (.) in front of a file name. In UNIX, each directory is subdivided into two directories: current directory (.) and parent directory (..). Attackers give a similar name like ". " (space is there, after .). These hidden files are usually placed in /dev, /tmp, /etc.

  An attacker can also edit the log files to cover their tracks. However, sometimes using this technique of hiding files, an attacker can leave his trace behind because the command he used to open a file with will be recorded in a .bash_history file. A smart attacker knows how to overcome such a problem; he does so by using export HISTSIZE=0 command.

Covering Tracks Tools

Track-covering tools help the attacker to clean up all the tracks of computer and Internet activities on the computer. They free cache space, delete cookies, clear Internet history, shared temporary files, delete logs, and discard junk.

- **CCleaner**

  Source: *https://www.piriform.com*

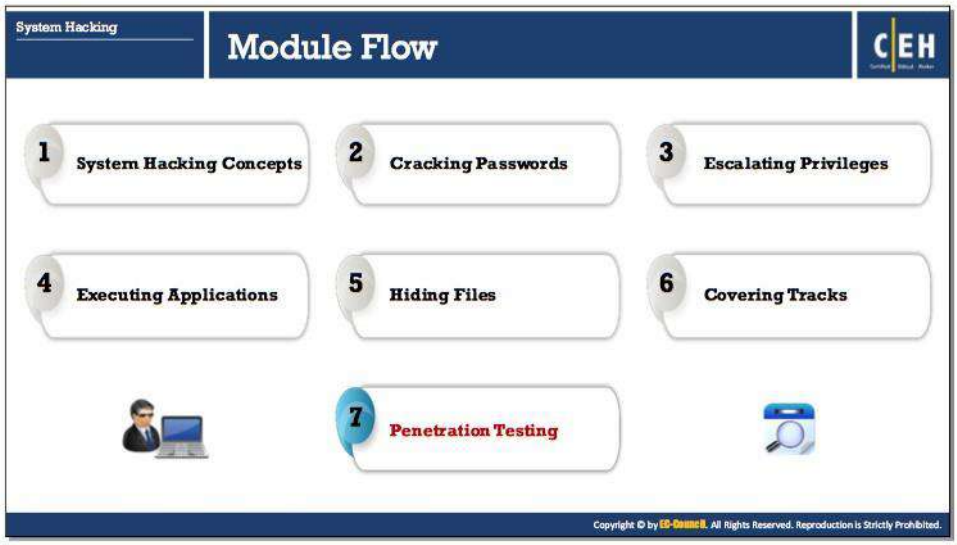
  CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the PC. It keeps your privacy online, and makes the system faster and more secure. In addition, it frees up hard disk space for further use. With this tool, an attacker can erase his/her tracks very easily. CCleaner also cleans traces of your online activities such as Internet history.

  It cleans the following areas of your Computer:

  - **Internet Explorer:** Temporary files, history, cookies, Autocomplete form history, index.dat.
  - **Firefox:** Temporary files, history, cookies, download history, form history
  - **Google Chrome:** Temporary files, history, cookies, download history, form history
  - **Opera:** Temporary files, history, and cookies
  - **Safari:** Temporary files, history, cookies, form history
  - **Windows:** Recycle Bin, Recent Documents, Temporary files and Log files.

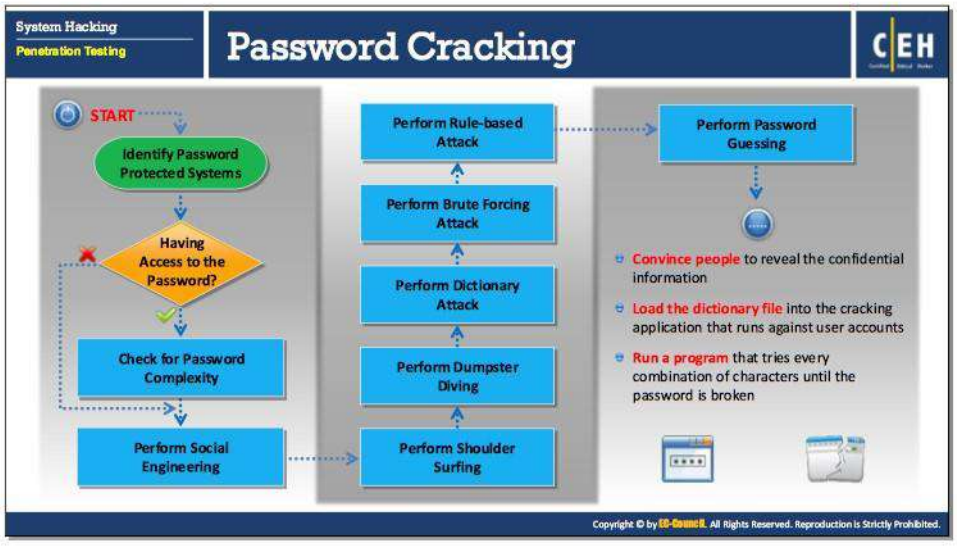
Some of the covering tracks tools are listed below:

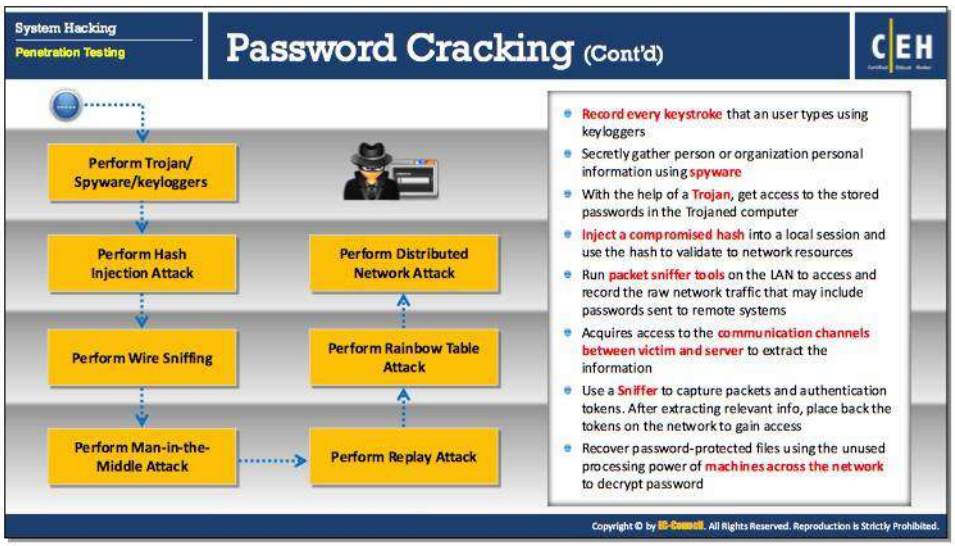
- DBAN (*http://www.cybertronsoft.com*)
- Privacy Eraser (*http://www.cybertronsoft.com*)
- Wipe (*https://privacyroot.com*)
- BleachBit (*https://www.bleachbit.org*)
- ClearProg (*http://www.clearprog.de*)
- AVG TuneUp (*https://www.avg.com*)
- Norton Utilities (*https://in.norton.com*)
- Glary Utilities (*http://www.glarysoft.com*)
- Clear My History (*https://www.hide-my-ip.com*)
- WinTools.net Professional (*http://www.wintools.net*)
- Free Internet Window Washer (*http://www.eusing.com*)

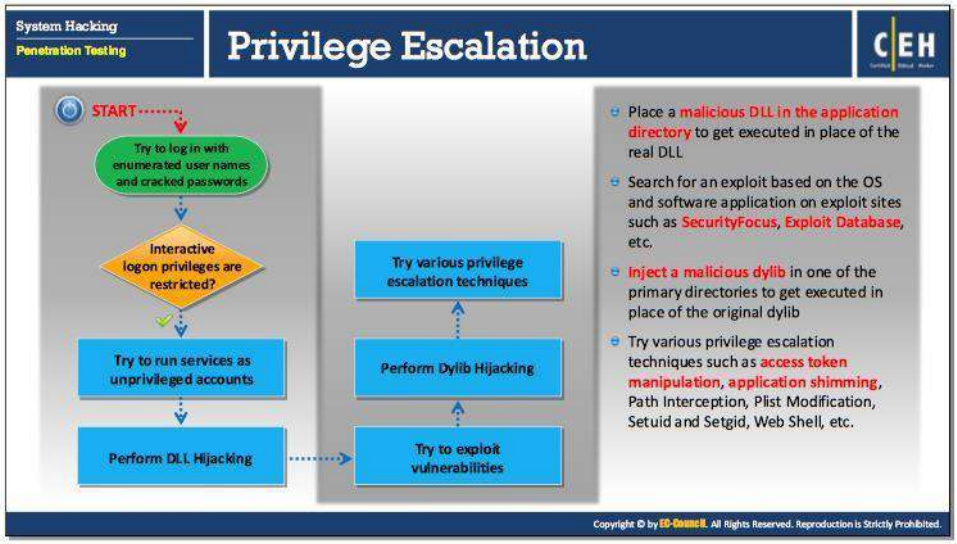


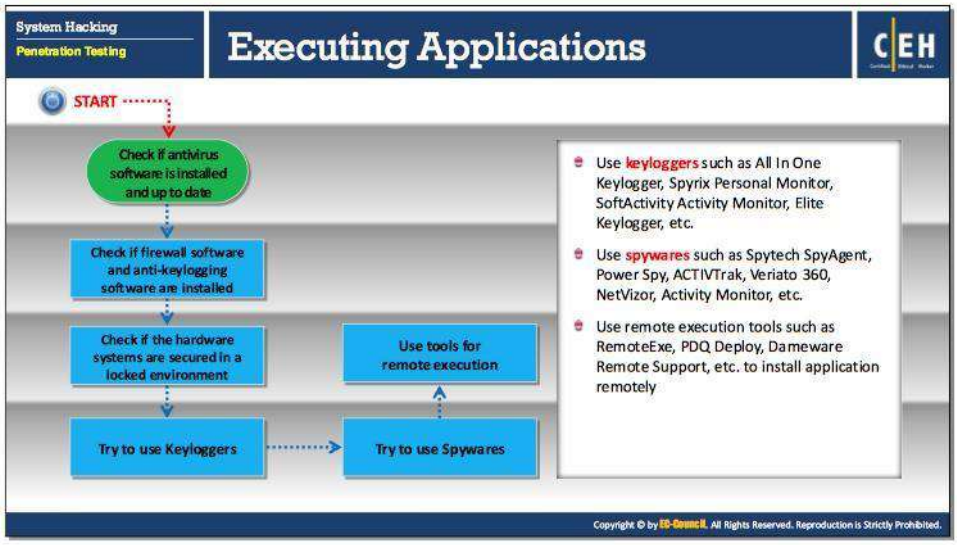
Penetration Testing

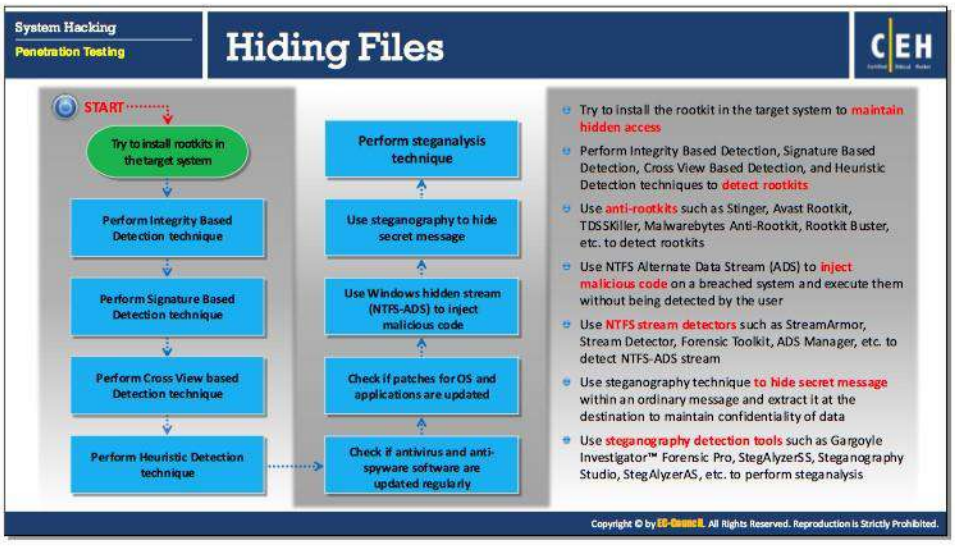
Pen testers use their system hacking knowledge to assess the security of target systems. As a pen tester, you should evaluate the security posture of your target system, by trying to break its security through simulating various attacks in the same way an outside attacker would do. There are certain steps you need to follow to conduct a system penetration test. This section will teach you how to conduct a system hacking pen test, with the help of knowledge gained through the CEH system hacking steps.

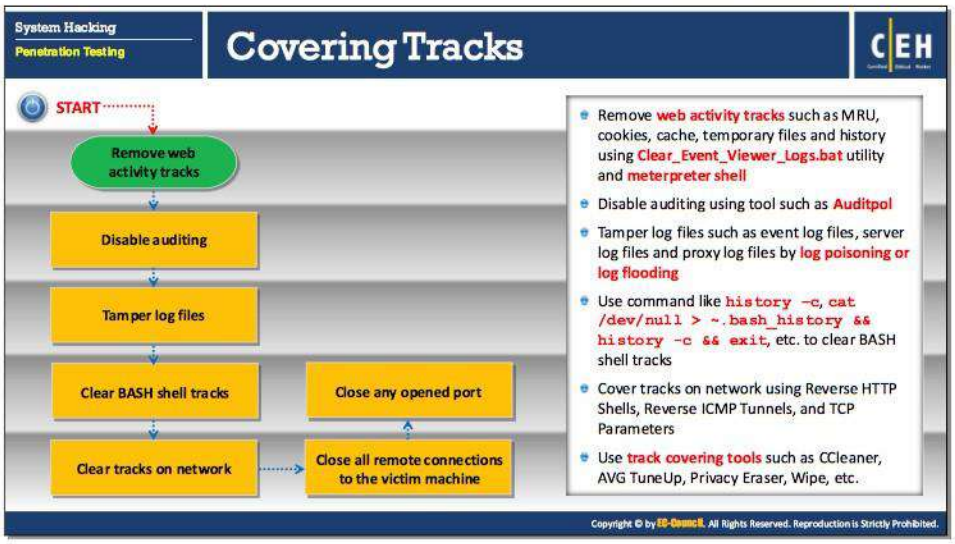


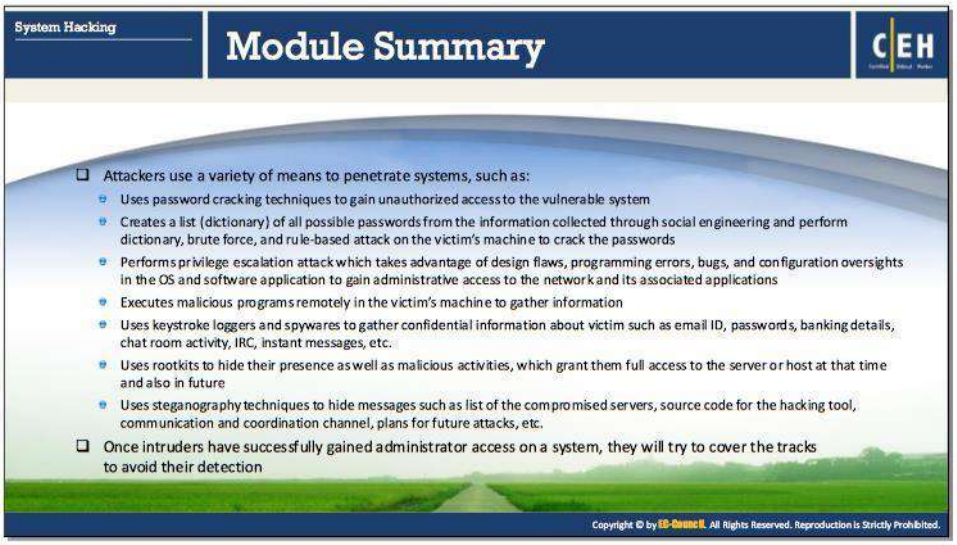












Module Summary

In this module, you have learned about the various tools, techniques, and methodology that hackers use to breach system security. Then we also explored the pen-testing steps for assessing target system security.