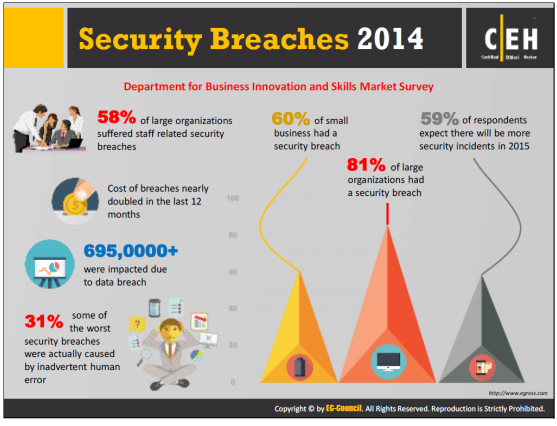
System Hacking

Module 05

Ethical Hacking and Countermeasures v9

Module 05: System Hacking

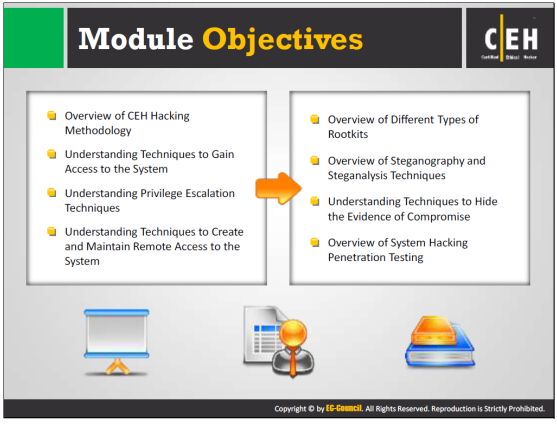
Exam 312-50



Egress Software Technologies—an encryption service provider—conducted a survey on Information Security Breaches. The survey mainly focuses on the data breaches and challenges facing organizations in 2014. Research shows there has been a significant rise in the cost of individual data breaches, as well as in the overall cost for all types of organization. The survey represents security breaches in 2014, as given below:

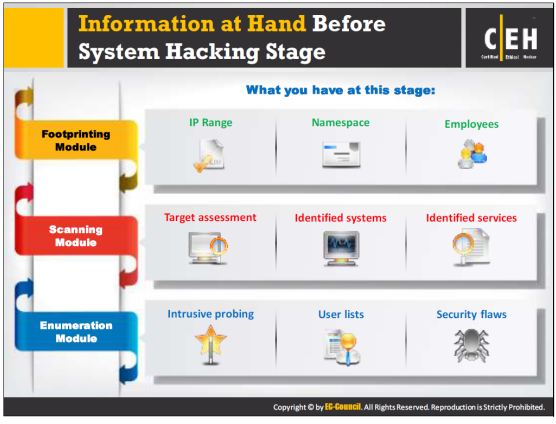
- 81% of large organizations had a security breach.
- 60% of small businesses had a security breach.
- 59% of respondents expect there will be more security incidents in 2015.
- 695,000+ were impacted due to a data breach reported in 2014.
- Cost of security breaches nearly doubled in the last 12 months.
  - The average cost of a data breach for a large organization (£600k–£1.15m; £450k–£850k in 2013; i.e., $886k–$1698k; $664k–$1255k in 2013)
  - The average cost of a data breach for a small organization (£65k–£115k; £35k–£65k in 2013; i.e., $96k–$170k; $52k–$96k in 2013)
- 31% worst security breaches were actually caused by inadvertent human error.
- 58% of large organizations suffered staff related security breaches.

Source: http://www.egress.com



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.



An attacker engages in system hacking attempts using information collected in earlier footprinting, scanning, and enumeration 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, 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.

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 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 perform malicious activities such as stealing sensitive data, implementing sniffer to capture network traffic, and infecting the system with malware.

- **Escalating Privileges**

  After gaining access to a system using a low-privileged normal user accounts, 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.

- **Executing Applications**

  Once attackers have administrator privileges, they attempt to install a malicious program 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.

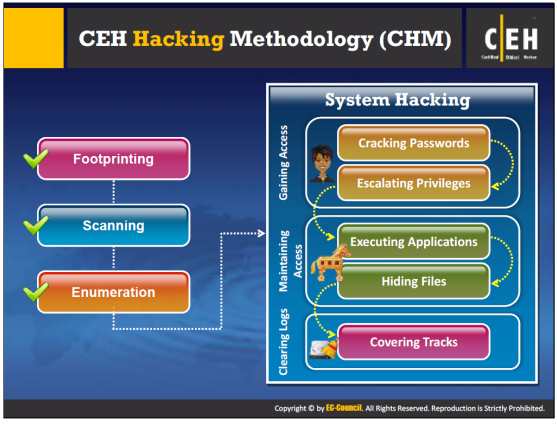
- **Hiding Files**

  Attackers use Rootkits 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.

Observe the diagram on the slide for a brief overview of objectives and techniques used, particularly during the hacking stage.



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**

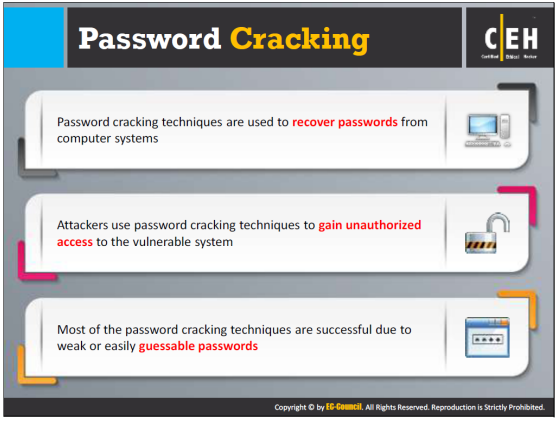
  After successfully gaining access to the target system, attackers work to maintain high levels of access to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files.

- **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 his activities in the system log, thus avoiding detection by users.

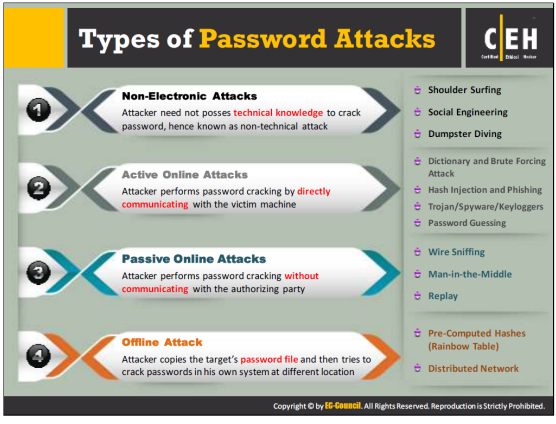
The figure in the slide shows steps and flow mechanisms between steps in the CEH Hacking Methodology (CHM).

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 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.



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.

- **Active Online Attacks**

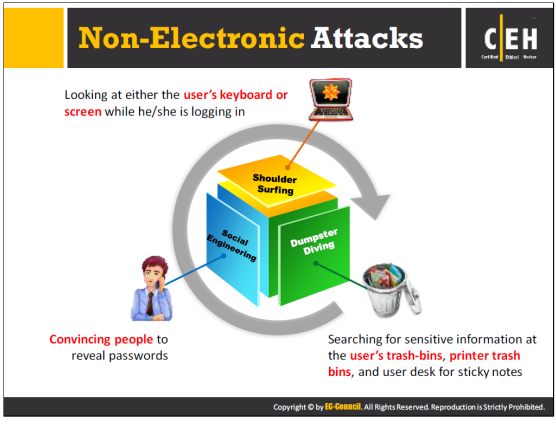
  This is one of the easiest ways to gain unauthorized administrator-level system access. An attacker needs to communicate with target machines to gain password access.

- **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.

Offline Attack

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.



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 trash cans, 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 into 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.

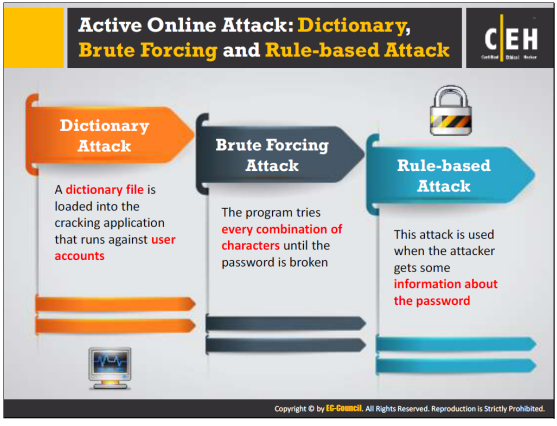
  This type of attack can also occur in a grocery store checkout line, when a potential victim is swiping a debit card and entering the required PIN (Personal Identification Number), which is typically only four digits, making it easier to observe.

- **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.



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**

  Attacker uses this type of attack when they obtain some information about the password. This is 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 to a minimum 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.

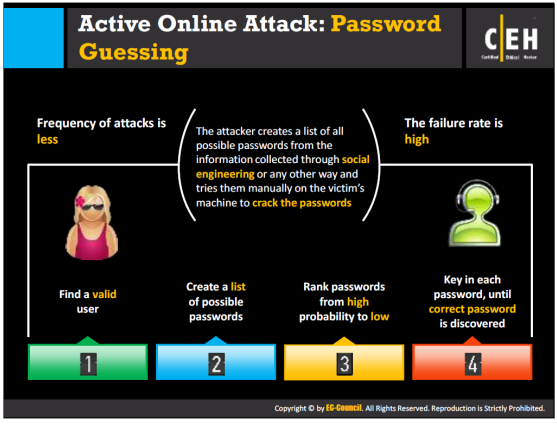
- **Hybrid Attack**

  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.



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.

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.

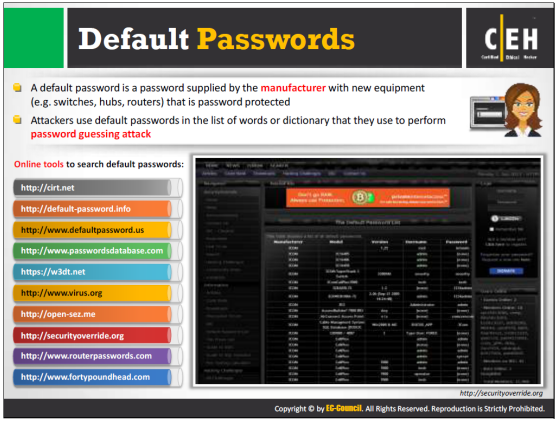
The main FOR loop can extract the user names and passwords from the text file, which serves as a dictionary as it iterates through every line:

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

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

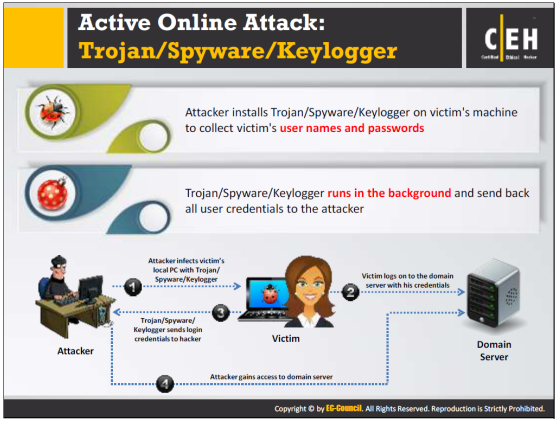
```
c:\>FOR /F "tokens=1,2*" %i in (credentials.txt)^
More? do net use \\victim.com\IPC$ %j /u:victim.com\%i^
More? 2>>nul^
More? && echo %time% %date% >> outfile.txt^
More? && echo \\victim.com acct: %i pass: %j >> outfile.txt
c:\>type outfile.txt
```

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 are those supplied by manufacturers with new equipment. Usually, default password 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 to successfully access the target device.

Source: http://securityoverride.org



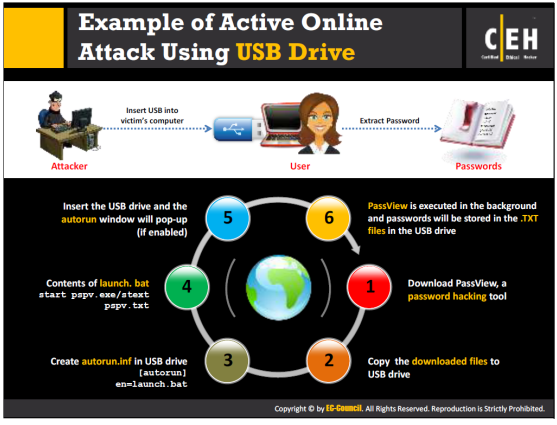
A Trojan is a program that masks itself as a benign application. The software initially appears to perform a desirable or benign function but instead steals information or harms the system. With a Trojan, attackers can gain remote access and perform various operations limited by user privileges on the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

For example, a key logger on a victim's computer is capable of revealing the contents of all user emails.

The picture in the slide depicts a scenario describing how an attacker gains password access using a Trojan/Spyware/Keylogger.



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.

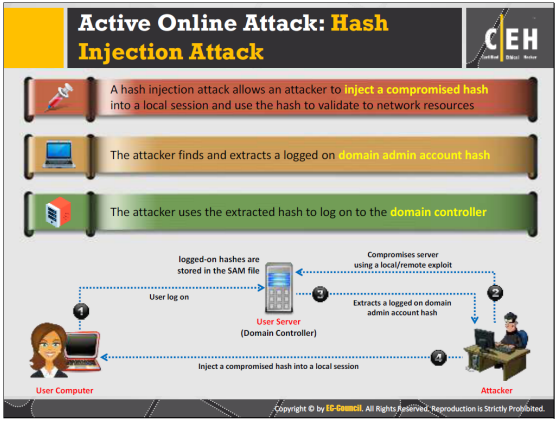
4. Open Notepad, and write the following content:

   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.



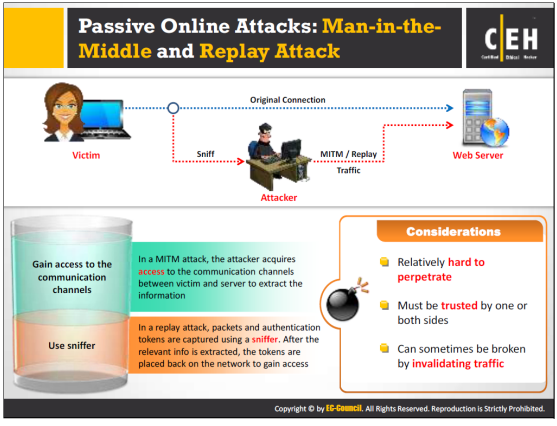
This type of attack is possible when the target system uses a hash function as part of the authentication process to authenticate its users. Generally, the system stores hash values of the credentials in the SAM database/file on a Windows computer. In such cases, the server computes the hash value of the user-submitted credentials or allows user to input 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, attackers inject a compromised hash into a local session and then use the hash to authenticate to the network resources. Hacker carry 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 any system with the same credentials.
- The hacker extracts all the hashes from the Active Directory database and can now compromise any account in the domain.

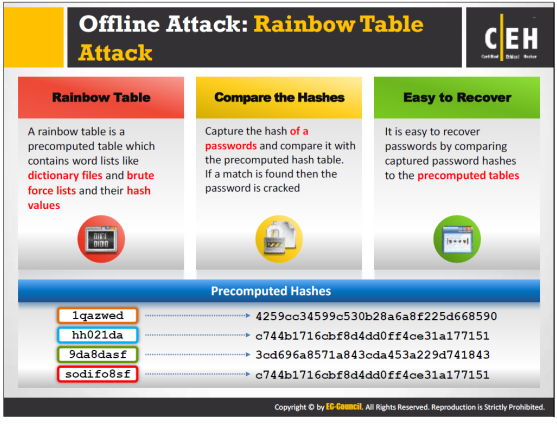
Packet sniffing is a form of wire sniffing or wiretapping in which hackers sniff the credentials during transit by capturing Internet packets. Attackers rarely use sniffers to carry out this type of attack. With packet sniffing, an attacker can gain passwords such as Email, websites, SMB, FTP, or SQL. 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 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. 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.



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. 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 communication. This method is relatively hard to perpetrate and can sometimes be broken by invalidating the traffic.

In a replay attack, a sniffer captures packets. After extracting the relevant information, the attacker places packets back on the network. 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 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 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 Attacks
2. Distributed network Attacks

Rainbow Attacks

A rainbow 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 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

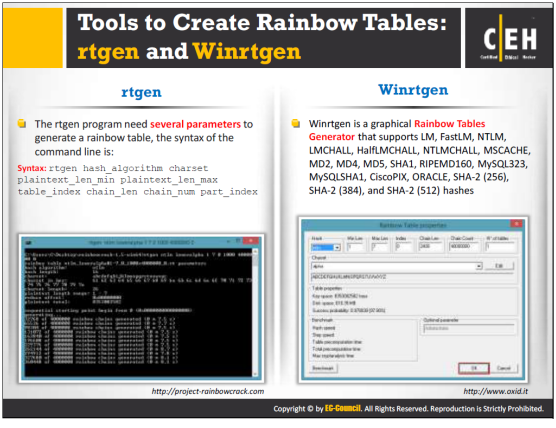
A rainbow table is a lookup table specially used in recovering a plaintext password from a cipher text. The attacker uses this table to look for the password and tries to recover it from password hashes.

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

It is easy to recover passwords by comparing captured password hashes to the pre-computed tables.



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.

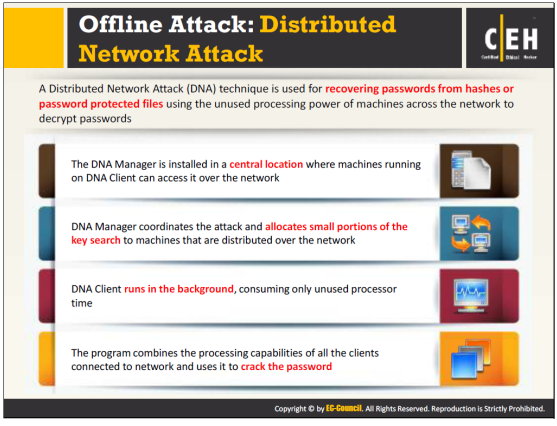
Winrtgen

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.

Generate Rainbow Tables Using Winrtgen:

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



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
- Controls the clients and identifies work done by clients

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.

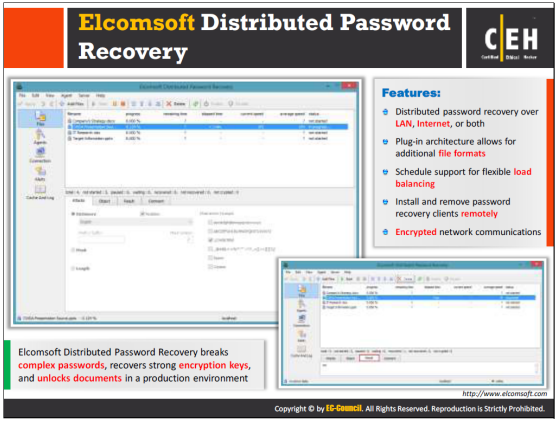
DNA Client Interface

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

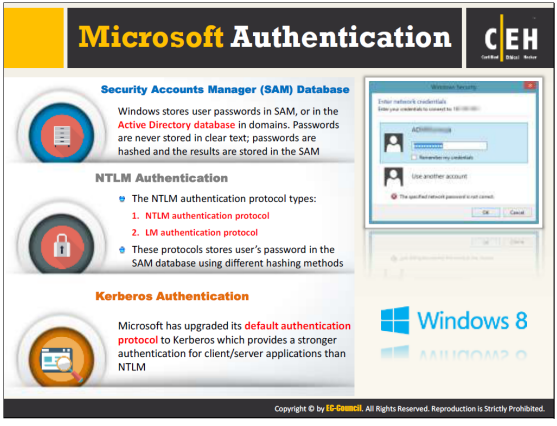
The Network Traffic dialog box aids in discovery of the network speed the DNA uses and each work-unit length of the DNA client. Using the work-unit length, a DNA client can work without contacting the DNA server. The DNA client application has the ability to contact the DNA server at the beginning and 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 traffic leads the client work on the jobs to spend longer amount of time. Therefore, the user can make fewer requests to the server because of the reduction in bandwidth of network traffic.



The Elcomsoft Distributed Password Recovery 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.

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



When users log in to the 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 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.

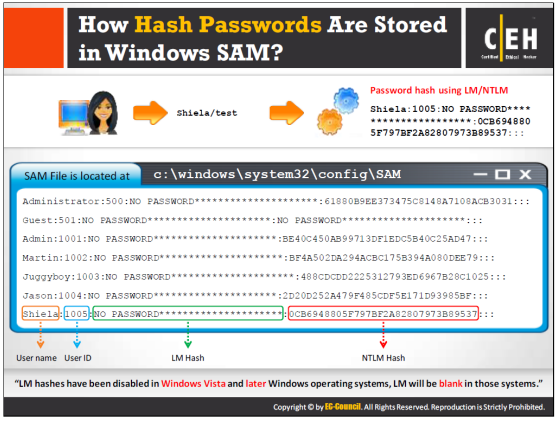
- **NTLM Authentication**

  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**

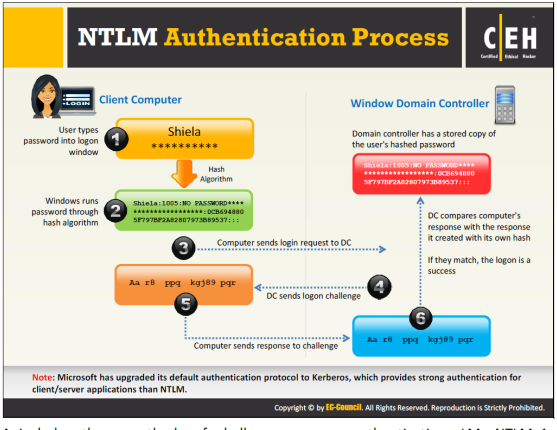
  Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography. This provides mutual authentication, in that both the server and the user verify each other's identity. Messages sent through Kerberos protocol are protected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



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.

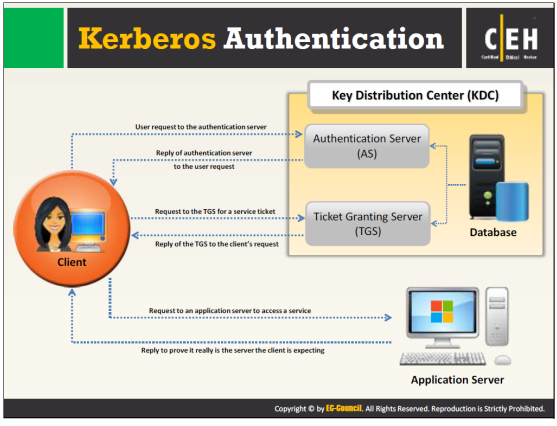
NTLM supersedes the LM hash, which is susceptible to cracking. New versions of Windows still support LM hashes for backward compatibility; however, Vista and later Windows versions disable LM hash by default. The LM hash is blank in newer Windows versions. Selecting the option to remove LM hashes enables 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 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).

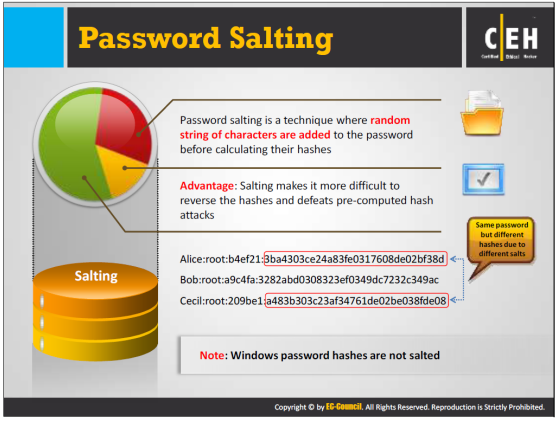
The following steps demonstrate the process and the flow of the client authentication to a domain controller using any NTLM protocol:

- 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 logon is success.



Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography, which provides 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.

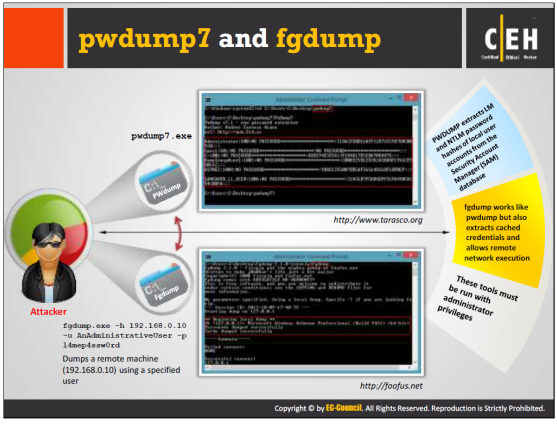
Kerberos makes use of the Key Distribution Center (KDC), a trusted third party, and consists of two logically distinct parts: an Authentication server (AS) and a Ticket Granting Server (TGS). The authorization mechanism of Kerberos provides the user with a Ticket Granting Ticket (TGT) that serves post-authentication 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.



"Salting" is a way of making passwords more secure by adding random strings of characters to them before their md5 hash is calculated. This makes cracking passwords more difficult. 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.



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

pwdump7

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

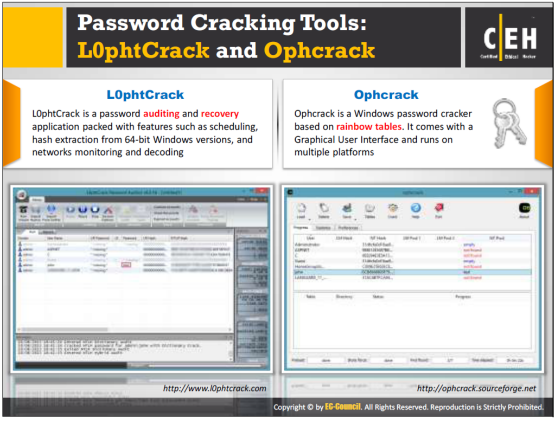
pwdump7 is an application that dumps the password hashes (One Way Functions or OWFs) from NT's SAM database. pwdump extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database. This application or tool runs by extracting the binary SAM and SYSTEM File 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.

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



Attackers can use the following tools to crack password of the target system:

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 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 that Locked, Disabled, Expired, or if the password is older than 180 days
- Delivers audit summary for 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
- Supports pull down menus change for language and character set

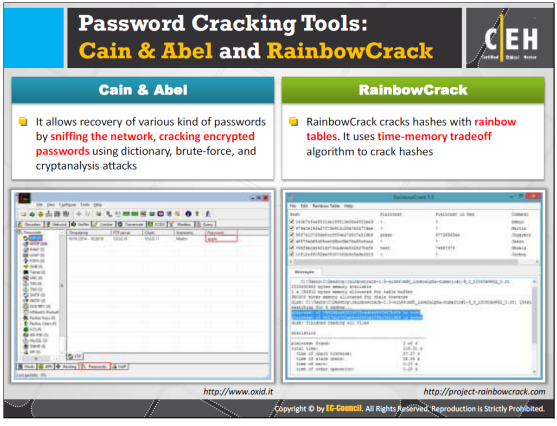
Ophcrack

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



Cain & Abel

Source: http://www.oxid.it

Cain & Abel is a password recovery tool that runs on the Microsoft operating system. It allows you to recover various kinds of passwords by sniffing the network, cracking encrypted passwords using a dictionary, brute-force and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. Cain & Abel tool recovers passwords and credentials from various sources easily.

It consists of APR (Arp Poison Routing), which enables sniffing on switched LANs and man-in-middle attacks. Its sniffer is also capable of analyzing encrypted protocols such as HTTPS and SSH-1, and contains filters to capture credentials from a wide range of authentication mechanisms.

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

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. List below are a few password cracking tools.

Offline NT Password & Registry Editor

Source: http://pogostick.net

Offline NT Password & Registry Editor is a utility to reset the password of any user that has a valid local account on the Windows system. This tool supports all versions of the Windows operating system. It works offline, that is, you have to shut down your computer and boot off a CD or USB disk to perform the password reset. In addition, this tool will detect and offer to unlock locked or disabled out user accounts. It contains a registry editor and other registry utilities that work under Linux/Unix, and it also helps in password editing.

Password Unlocker Bundle

Source: http://www.passwordunlocker.com

Password Unlocker Bundle is a password recovery tool allows you to reset and recover login or open passwords for 60 applications or file types, including Windows OS, MS SQL Severs, RAR/ZIP archives, PDF, MS Word/Excel/PPT files, MS Office 2010, among others.

Proactive System Password Recovery

Source: http://www.elcomsoft.com

Assuming that the user has logged into the system, Proactive System Password Recovery can retrieve various passwords such as Windows logon, .NET, screensaver, RAS and dial-up, VPN (Virtual Private Network) connections, and access rights to shared resources. This tool employs an advanced social engineering technology to retrieve all recoverable passwords and try these passwords when unlocking secure ones. It adds the discovered passwords automatically to a dictionary and performs a dictionary attack that is faster than brute-force recovery.

John the Ripper

Source: http://www.openwall.com

John the Ripper is a password cracker, which is currently available for many flavors of UNIX, Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak UNIX passwords. Besides several crypt (3) password hash types most commonly found on various Unix systems, supported out of the box are Windows LM hashes, as well as many other hashes and ciphers in the community-enhanced version.

Windows Password Cracker

Source: http://www.windows-password-cracker.com

Windows Password Cracker is password recovery software that extracts Windows user names and passwords in national symbol encoding. It supports brute-force and dictionary password recovery attacks.

WinPassword

Source: http://lastbit.com

WinPassword (formerly, NT Password) is an application for Windows system administrators used to find breaches in system security. It tries to recover plain-text passwords by analyzing user password hashes. If it is possible to recover a password within a reasonable amount of time, the password is considered insecure. Windows Password helps to recover lost passwords of particular users.

Passware Kit Enterprise

Source: http://www.lostpassword.com

Passware Kit Enterprise recovers passwords for more than 200 file types and decrypts hard disks providing an all-in-one user interface. It also includes Encryption Analyzer, which scans computers for password-protected files. This tool supports batch file processing and distributed and cloud-computing password recovery for both Windows and Linux platforms.

PasswordsPro

Source: http://www.insidepro.com

Password Pro is a software tool for recovering passwords to hashes, and it features the following:

- Supports over 210 hashing algorithms
- Supports plugins usage
- Allows editing of hashes and other data
- Exports hashes to text or HTML file
- Verifies hashes and their passwords
- Recovery of passwords

LSASecretsView

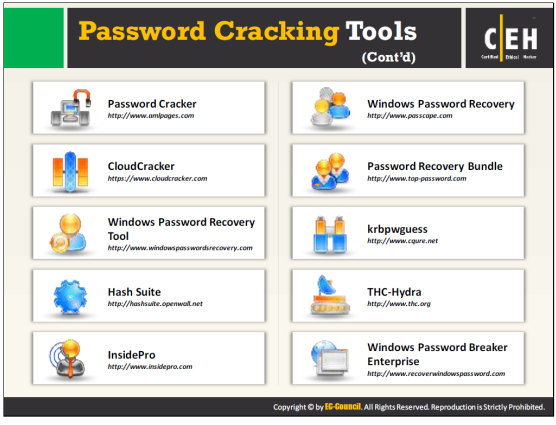
Source: *http://www.nirsoft.net*

LSASecretsView is a utility that displays the list of all LSA secrets stored in the computer's Registry. The LSA secrets key is located in HKEY_LOCAL_MACHINE\Security\Policy\Secrets and may contain your RAS/VPN passwords, Autologon password, and other system passwords/keys.

LCP

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

LCP tool allows auditing of user account passwords and recovery in Windows systems by importing accounts information from the local computer, remote computer, SAM file, .LC file, .LCS file PwDump file, or Sniff file.



Below is the list of some recognized password cracking tools used by attackers.

Password Cracker

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

Password Cracker is a tool that restores forgotten passwords. It works on Internet Explorer. To extract the password, just hover the mouse over the asterisks (or other symbols) displayed at the password location to see the actual password.

CloudCracker

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

An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption.

Windows Password Recovery Tool

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

Windows password recovery software is a tool to recover any Windows password. It works offline to recover, reset, unlock, bypass, change Windows password. This tool has four versions, offering more options to reset your password.

Hash Suite

Source: http://hashsuite.openwall.net

Hash Suite is a Windows program for testing the security of password hashes that is used by system administrators, IT security personnel, and IT security consultants.

InsidePro

Source: http://www.insidepro.com

InsidePro Software is a professional password recovery suite that gives detailed descriptions of various hashing algorithms and checksums, and information on the application of certain algorithms and applications that support such hashes.

Windows Password Recovery

Source: http://www.passcape.com

Windows Password Recovery is a Windows password recovery utility and a network security analyzer that implements advanced password recovery technologies such as Artificial Intelligence or Pass-phrase attack.

Password Recovery Bundle

Source: http://www.top-password.com

The Password Recovery Bundle tool is used to recover all lost or forgotten passwords. It recovers or resets passwords for Windows systems, PDF, ZIP, RAR, Office Word/Excel/PowerPoint documents, and Lost CD key. It also retrieves passwords for all popular instant messengers, email clients, web browsers, FTP clients, VNC, Remote Desktop Connection, Total Commander, Dialup, and many other applications.

krbpwguess

Source: http://www.cqure.net

krbpwguess is, as its name suggests, a Kerberos password-guessing tool. Built against the Heimdal Kerberos libraries, the tool works on Snow Leopard and Ubuntu Linux. It reads a file of user names, against which it guesses a dictionary with passwords. After finding a match, it logs to the screen or to a supplied output file. The tool relies on Kerberos being setup properly, either through DNS or with the appropriate entries in the krb5.conf configuration file. Both the user and the password file should contain a single entry per line, and should work with both UNIX and Windows line breaks.

THC-Hydra

Source: http://www.thc.org

THC-Hydra is a network logon cracker that supports many different services, such as IPv6 and Internationalized RFC 4013. It comes with a GUI and supports HTTP proxy and SOCKS proxy. THC-Hydra utilizes various authentication methods for services, including Firebird, FTP, IMAP, LDAP, MS-SQL, RDP, SMTP, SNMP, and Telnet.

Windows Password Breaker Enterprise

Source: http://www.recoverwindowspassword.com

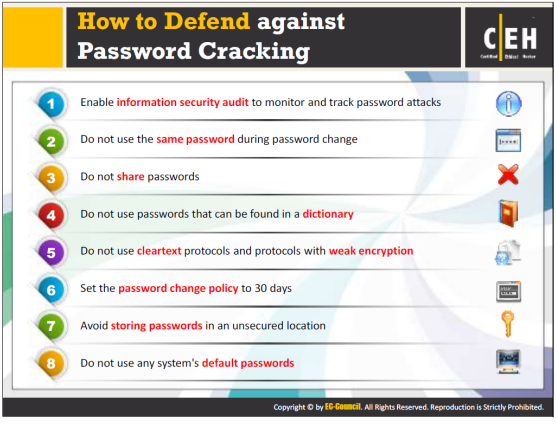
Windows Password Breaker Enterprise helps to reset local administrator and other user passwords on all popular Windows platforms. It also can reset a domain administrator password on Windows Server 2008(R2)/2003(R2), which act as a domain controller. This tool can reset Windows passwords by creating a password reset disk via CD/DVD or a USB drive.

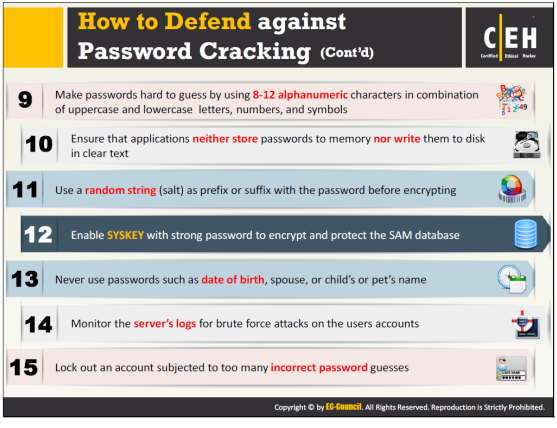
FlexiSPY Password Grabber can capture the security pattern of the phone itself and crack the passcode used to unlock the iPhone, plus the actual passwords they use for social messaging, emails, and applications. It allows you to login to others Facebook, Skype, Twitter, Pinterest, LinkedIn, and Gmail and other Email accounts directly from your tablet, mobile phone, or computer. By installing FlexiSPY's Android Password Grabber on a new phone before configuring other apps, one can find every password on the phone.

Features:

- Uses an intuitive, simple design to easily display all account activity
- Captures the device's drawn security pattern for direct access to it, and if the pattern changes, the user receives an update
- If a password changes, FlexiSPY will be updated with the new one
- Ability to share passwords with other interested parties without their having access to your FlexiSPY account

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





Additional best practices to protect against password cracking include:

- 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.

A strong security policy provides the foundations for the successful implementation of future security-related projects. This is the first measure to implement for reducing the risk of objectionable use of any of the company's information resources. The first step towards augmenting a company's security is the introduction and implementation of an accurate yet enforceable security policy. It provides "Do's" and "Don'ts" to secure a network, system, or resources.

The proper implementation of a security policy not only helps you to reduce risk of compromising, but also helps in the company's effort to secure its communications.

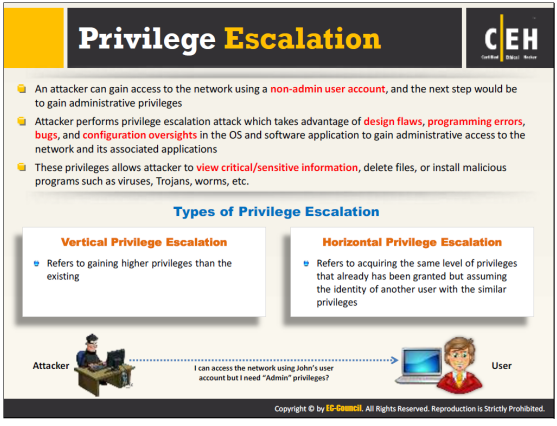
Additionally, the implementation process of a security policy will also help define a company's critical assets and the ways to protect them, and will serve as a centralized document for protecting security assets.

Characteristics of good security policy:

- The security policy should be flexible enough to adopt the changing requirements.
- It should set standards and guides users for acceptable use.
- The policy should be unambiguous and easy to understand.
- The policy should balance enforcement and productivity; otherwise, it will be useless.

The diagram shown in the slide is an example of Permanent Account Lockout-Employee Privilege Abuse policy for users who perform prohibited activities, as per the security policy enforced by an organization.

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 slides explain various tool and techniques attackers use to escalate their privileges.



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 gain access to the networks and its associated data and applications by taking advantage of defects in design, software application, poorly configured operating systems, and so on.

Once an attacker has gained access to a remote system with a valid user name 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.

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.

Types of Privilege Escalation

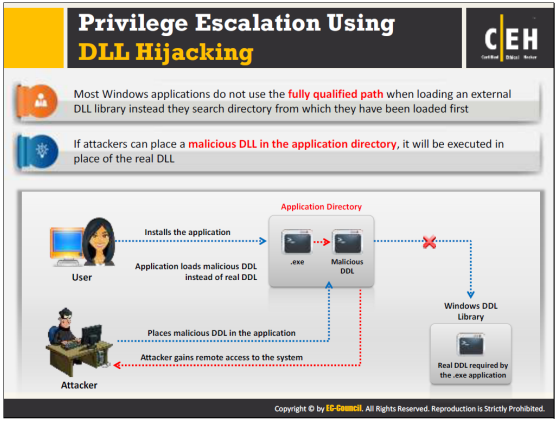
There are two types of privilege escalation: horizontal and vertical.

- **Horizontal Privilege Escalation**

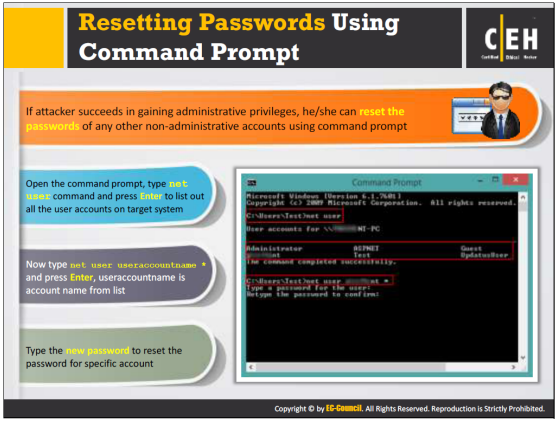
  In a horizontal privilege escalation, the unauthorized user tries to access the resources, functions, and other privileges that belong to the authorized user who has similar access permissions. For instance, online banking user A can easily access user B's bank account.

- **Vertical Privilege Escalation**

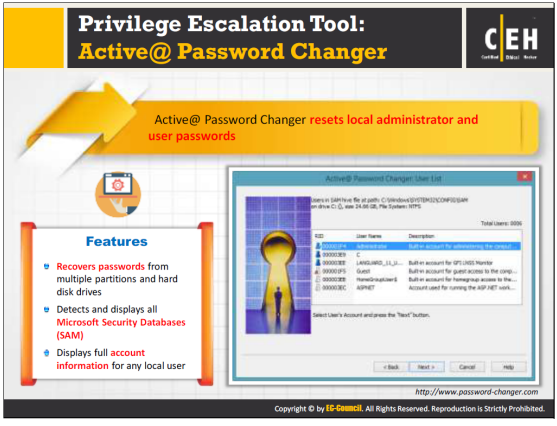
  In a vertical privilege escalation, the unauthorized user tries to gain access to the resources and functions of the user with higher privileges, such as application or site administrators. For example, someone performing online banking can access the site using administrative functions.



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.



The password of the any non-administrative user account on the system can be easily reset from a command prompt, assuming you have the administrative account privileges on the same system. An attacker may take the advantage of this feature to deprive owners of user accounts from accessing the system, and will perform malicious activities through the users' Windows identities.



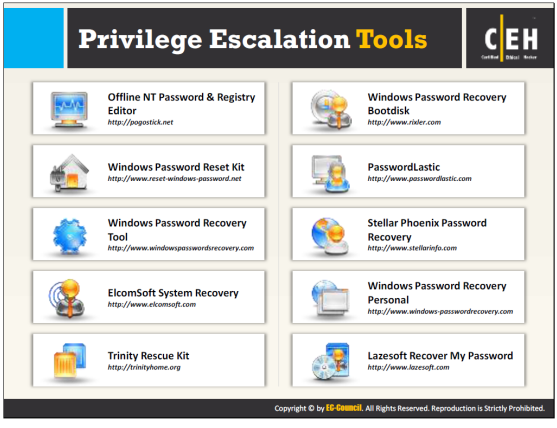
Active@Password Changer is a password recovery tool that resets the local administrator and user passwords when the administrator has lost or forgotten his/her password, or if the system locks out or disables the administrator's user account.

Features:

- Recovers passwords from multiple partitions and hard disks
- Detects and displays all Microsoft Security Databases
- Displays all local users
- Displays full account information for any local user
- Resets administrator's/user's password
- Resets "User is Disabled" flag
- Disable Force Smart Card Login
- Can run from bootable floppy, CD, or USB Flash
- Windows Bootable Disk Creator allows to create bootable disks in different formats—CD/DVD/Blu-ray, USB-flash, or an ISO image
- Ability to change (set or clear) user's account flags: "User must change password at next logon," "Password never expires," "Account is disabled," "Account is locked out"
- Ability to manage logon time (Permitted logon hours) for a local user

- Supports FAT16, FAT32, exFAT, NTFS, NTFS5 file systems
- Supports large hard-disk drives (greater than 2TB)
- Supports IDE SATA eSATA SSD and SCSI hard disks
- Old operations systems supported: DOS version for MS-DOS, PC-DOS, DR-DOS, FreeDOS, OpenDOS, and Windows 95/98/ME

Source: *http://www.password-changer.com*



A few privilege escalation tools are discussed below.

Offline NT Password & Registry Editor

Source: *http://pogostick.net*

Offline NT Password & Registry Editor is a utility for resetting the password of any user that has a valid local account on your Windows system. This tool allows setting up a new password without having to know the old one.

Windows Password Reset Kit

Source: *http://www.reset-windows-password.net*

Windows Password Reset Kit is a password reset bootdisk to safely remove, reset, or bypass Windows administrator and user passwords. Boot Windows Password Reset Kit from a CD/DVD or USB flash drive and gain access to your locked computer by resetting the forgotten or unknown password to blank.

Windows Password Recovery Tool

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

Windows password recovery software helps you recover Windows password without reinstalling the system. With this tool, you can reset the forgotten passwords for local administrator and other user accounts on a Windows OS (e.g., recover a Windows 8 password).

It offers two options for creating a Windows password reset disk, making sure that you can boot up any desktop or laptop when you cannot run Windows.

ElcomSoft System Recovery

Source: http://www.elcomsoft.com

ElcomSoft System Recovery restores access to locked windows accounts by recovering or resetting Windows system passwords. This tool unlocks locked and disabled user and administrative accounts in all versions of Windows.

Trinity Rescue Kit

Source: http://trinityhome.org

Trinity Rescue Kit or TRK is a free live Linux distribution that aims at recovery and repair operations on Windows machines, but is equally usable for Linux recovery issues. It allows performing maintenance and repair on a computer, ranging from password resetting over disk cleanup to virus scanning. It resets Windows passwords with the winpass tool.

Windows Password Recovery Bootdisk

Source: http://www.rixler.com

Windows Password Recovery Bootdisk allows logging into your account even if you have forgotten the password, and by recovering the hash of the original password, it allows you to restore it. The program records a bootable USD stick or CD/DVD disk and loads the system from it. After that, it removes a password of the specified user or all of them, thus allowing you to log into those accounts, and it recovers hash data for further retrieval of lost passwords.

PasswordLastic

Source: http://www.passwordlastic.com

Windows Password Recovery Lastic from PasswordLastic's Password Recovery Tools allows you to restore access to your system if you lost or forgot your Windows password. Run it on another computer to create a bootable USB stick or CD/DVD disk. Boot from it on your computer, and it will list all user accounts it finds, offering you an easy way to remove a password for any of them. In addition, it supports saving password hashes for in-depth cracking, and restoring of previously removed passwords.

Other than Windows Password Recovery Lastic, PasswordLastic's also provides tools to crack passwords in MS office, MS excel, MS word, MS VBA, MS outlook, and others.

Stellar Phoenix Password Recovery

Source: http://www.stellarinfo.com

Stellar Phoenix Password Recovery tool resets passwords of all administrator and user login accounts on Windows 7, Vista, and XP. This software performs Windows password recovery for various email clients, FTP clients, web browsers, and chat messengers installed on your computer.

Windows Password Recovery Personal

Source: http://www.windows-passwordrecovery.com

Windows Password Recovery Personal 2013 recovers the forgotten Windows password and domain password for Windows. You can also create a new Administrator account, regain access to Windows system in minutes by burning a bootable CD/DVD, or USB flash drive.

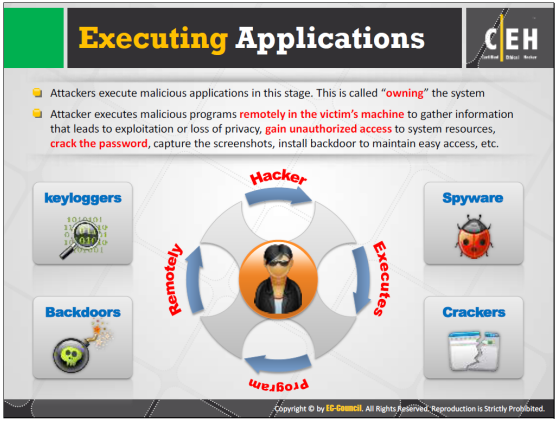
Lazesoft Recover My Password

Source: http://www.lazesoft.com

Lazesoft Recover My Password is a Windows password recovery tool used to remove Windows logon password, reset Windows password to blank, unlock, and enable your locked or disabled user account. It can reset passwords bootable CD/DVD and USB Drive, local Administrator password, and so on.

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.

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.

RemoteExec is a remote administration tool that helps attackers perform various malicious activities on target systems. Having gained administrative privileges, attackers use this tool to install, execute, delete, and/or modify the restricted resources on the victim machine.

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 want 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 launched 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.

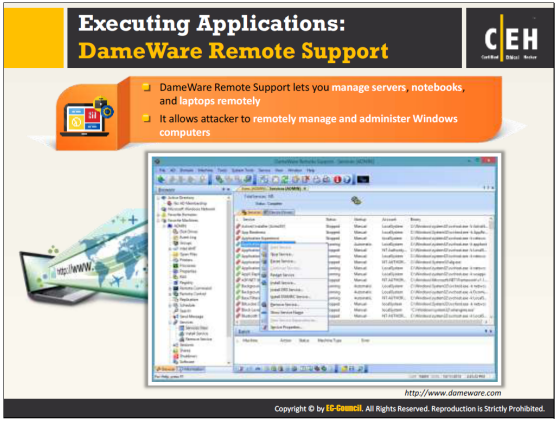
Source: *http://www.isdecisions.com*

PDQ Deploy is a software deployment tool with which you can easily install almost any application or patch to your computer. This tool helps to deploy the MSI, MSP, MSU, EXE, and batch installers to numerous Windows computers at the same time. You can quickly deploy a packaged program to the selected or to all computers on your network. The features of PDQ Deploy include that it integrates with Active Directory, Spiceworks, PDQ Inventory, and installs to multiple computers simultaneously, as well as real-time status.

Salient features:

- Install MSIs to multiple computers
- Install EXEs to multiple computers
- Ready-to-deploy Installs in the package library
- Customize the installs

Source: http://www.adminarsenal.com

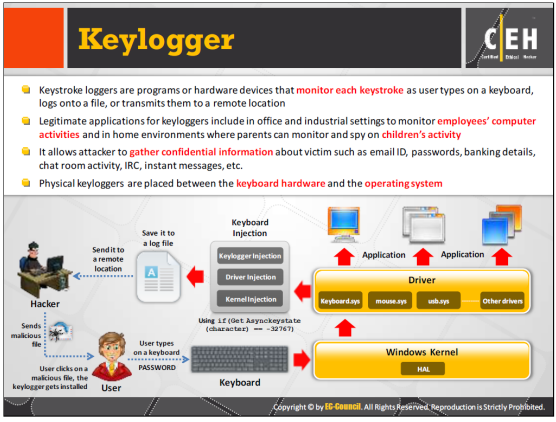


DameWare Remote Support (DRS) is a remote system administration tool that includes remote control software, Mini Remote Control, and the DameWare Central Server for advanced management and secures remote connections to computers outside the firewall. DRS offers flexible deployment options, allowing you to choose which components to install.

Features:

- Perform Windows administration tasks remotely
- Remotely control desktops, laptops, and servers
- Securely access computers outside the firewall
- Centrally manage users, licenses, and host lists
- Manage multiple active directory domains
- Support end users from your iOS or Android device

Source: http://www.dameware.com



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.

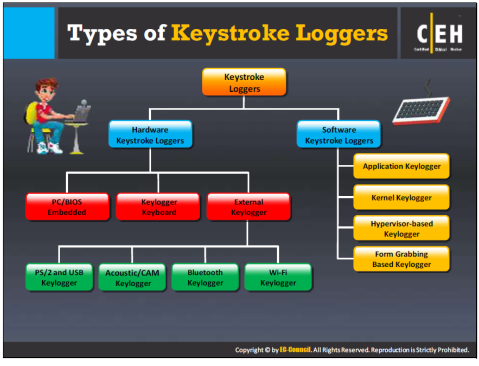
A keylogger, when associated with spyware, helps to transmit your information to an unknown third party. Attackers use it illegally for malicious purposes such as for stealing sensitive and confidential information about victims. The sensitive information includes email IDs, passwords, banking details, 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. 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



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 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 the data such as emails, chat records, applications used, IMs, and so on.
  - **Acoustic/CAM Keylogger:** 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 installing 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 keyloggers work 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.

Acoustic/CAM Keylogger

Acoustic keyloggers work on the principle of converting electromagnetic sound waves into data. The concept is that each key on the keyboard makes a slightly different sound when it is pressed. There are listening devices that are capable of detecting the subtle variations between the sounds of each keystroke and use this information to record the target's keystrokes.

The acoustic keylogger requires a "learning period" of 1,000 or more keystrokes to convert the recorded sounds into the data. To determine which sound corresponds to which key, the acoustic keylogger uses statistical data based on the frequency of the keystrokes, as people use some letters much more than others.

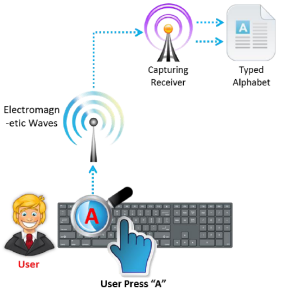


FIGURE 5.1: Screenshot showing the working of Acoustic Keylogger

In webcam keylogging, attackers make use of a webcam to record the keysokes. The cam installed takes screenshots of the keystrokes and sends the recorded screenshots to the attacker. The attacker can retrieve the keystroke information by probing the screenshots sent by the webcam.

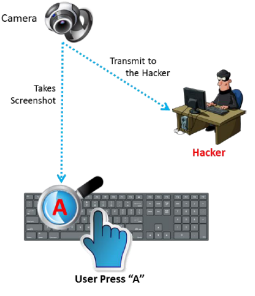


FIGURE 5.2: Screenshot showing the working of CAM Keylogger

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:

- 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.

FIGURE 5.3: Screenshot showing different types of hardware Keyloggers

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

KeyGrabber

Source: http://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.

KeyGhost

Source: http://www.keyghost.com

The KeyGhost Hardware Keylogger is a tiny plug-in device that records every keystroke typed on any PC computer. It records and retrieves everything typed, including emails, chat room activity, instant messages, website addresses, search engine searches, and more with plug-in keylogger.

KeyCobra

Source: http://www.keycobra.com

The KeyCobra hardware keylogger is a small device that, once plugged in between keyboard and computer, records all keystrokes typed. These devices are dual-function: a keystroke recorder and a flash disk for instant data retrieval. There are no software drives required—it is simply "plug and play." KeyCobra is completely undetectable to antivirus software and firewalls.

FIGURE 5.4: Screenshot of Hardware Keylogger - KeyCobra

KeyKatcher

Source: *http://keykatcher.com*

The KeyKatcher hardware keylogger is a device used to record keystrokes typed on the target system. It also comes in different versions, such as KEYKatcher Professional–USB Drive, KeyKatcher 64K Mini PS/2 Hardware Keylogger, and so on.

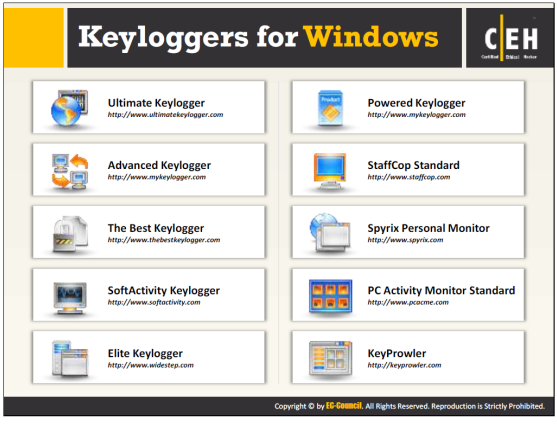
FIGURE 5.5: Screenshot of Hardware Keylogger – KeyKatcher

All In One Keylogger is 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 Al In One Keylogger:

- Capture all keystrokes (keystrokes logger)
- Record instant messages
- Monitor application usage
- Capture desktop activity
- Capture screenshots
- Quick search over the log
- Send reports via email, FTP, network
- Record microphone sounds
- Generate HTML reports
- Disable anti keyloggers
- Disable unwanted software
- Filter monitored user accounts

- Send reports in HTML format
- Block unwanted URLs
- Stop logging when the computer is idle

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



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.

Ultimate Keylogger

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

Ultimate Keylogger is an application that monitors all activities on computer systems, including applications, keystrokes, passwords, clipboard contents, chat, email, and websites visited. It sends encrypted activity reports invisibly via email, FTP, or network.

Advanced Keylogger

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

Advanced Keylogger collects complete reports of users' activity. You can easily discover keystrokes, websites visited, and clipboard contents. It also controls all outgoing IM conversations. Advanced Keylogger does all this while remaining absolutely invisible to the system.

The Best Keylogger

Source: http://www.thebestkeylogger.com

The Best Keylogger logs all keystrokes, mouse clicks, applications, windows, websites, email sent and received, chat conversations, system events, documents printed, file usage, and screenshots. It can also be filtered to log only specific users and specific applications, and deny access to specified applications and websites. The Best Keylogger can email you all the logs, so you can monitor your computer without your being present. It provides encrypted logs that it will decrypt and display only after you enter your admin password.

SoftActivity Keylogger

Source: http://www.softactivity.com

SoftActivity keylogger is software that runs invisibly in the background and secretly records all URLs visited, keystrokes, chat conversations, emails sent and received, programs run, and so on. It can capture screenshots of remote desktops at preset times. All recorded keylogger information is stored in an encrypted log file. You can set up SoftActivity Keylogger to send the reports to your mailbox every few hours.

Elite Keylogger

Source: http://www.widestep.com

Elite Keystroke records all keystrokes typed, remaining completely undetectable to users. Elite Keylogger lets you know what was typed (passwords, logins, addresses, names), in which applications, and who typed it. It records all application activities, monitors websites visited, provides multiple log delivery options, and so on.

Powered Keylogger

Source: http://www.mykeylogger.com

Powered Keylogger is an invisible keylogger that operates deeply in the system and provides a maximum stealth level. In addition to its primary key-capture function, it acts as a full-fledged computer monitoring tool.

StaffCop Standard

Source: http://www.staffcop.com

StaffCop Standard has a built-in key logger that records user passwords for social networks and other login-only websites. It also allows you to monitor all activities on company computers and prevent unauthorized distribution of sensitive corporate information. It enables you to prevent, detect, respond, monitor, and review measures to reduce perceived risk of corporate data loss.

Spyrix Personal Monitor

Source: http://www.spyrix.com

Spyrix Personal Monitor is a powerful multifunctional program for complete and detailed remote monitoring of user activity. It can monitor keystrokes, activity on social networks (e.g., Facebook, MySpace), web-surfing, Skype and IM (e.g., ICQ, MSN) communications, running and

active applications, printing activity, and external storage (e.g., USB, CD, DVD, HDD, memory cards).

PC Activity Monitor Standard

Source: http://www.pcacme.com

The PC Activity Monitor (PC ACME) line of applications is currently in its 7.x version and works under 32-bit versions of Windows 2000 and Windows XP operating systems. All user data are monitored and collected invisibly by the "agent" and saved to a hidden, encrypted log file located on the monitored PC.

KeyProwler

Source: http://keyprowler.com

KeyProwler allows you to record and control everything that happens on your computer and have it delivered to your email address daily, including applications used, time stamps, clipboard data, and screenshots.

The following useful keyloggers also run on the Windows operating system:

Keylogger Spy Monitor

Source: *http://ematrixsoft.com*

Keylogger Spy Monitor spy software can secretly record all keystrokes, including data such as chats, usernames, passwords, emails, search queries, and other content. It works in stealth mode, making it completely invisible, even to a skilled PC user. When required, the program can be revealed using hotkeys. You can check logging reports by receiving emails or opening a web page.

REFOG Personal Monitor

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

REFOG Personal Monitor is software that records PC user's actions, grabs screenshots, and records keystrokes. For example it allows parents to monitor children's activities remotely over the Internet and runs in stealth mode while capturing chats and instant messengers. It also provides real-time alerts.

Actual Keylogger

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

Actual Keylogger allows you to discover what other users might do on your computer in your absence. Designed for hidden computer monitoring of such activity, Actual Keylogger is capable

of catching all keystrokes; capturing the screen; logging running and closed programs, and websites visited; and monitoring clipboard contents.

Spytector

Source: http://www.spytector.com

Spytector tracks all the activities of PC users (e.g., keystrokes, usernames and passwords, visited websites, opened windows, applications) in complete stealth mode, and delivers the logs to you via Email or FTP. It allows you to monitor only specific window applications or visited websites by creating a keylogger filter to monitor only required information.

KidLogger

Source: http://kidlogger.net

KidLogger collects data about user activity on the Computer or mobile phone, and creates detailed time-tracking and productivity reports available online. As its name implies, it is designed primarily to be used by parents to monitor children's computer use. However, it is also useful for monitoring the activities of adults.

Features:

- Informs parents regarding children's computer (PC or Mac) use.
- Creates a list of most used apps and web sites
- Employee time tracking and workplace productivity tracking
- Displays the most-used phone contacts (e.g., calls, SMS, chats)

Micro Keylogger

Source: http://www.microkeylogger.com

Micro Keylogger (also called a keystroke logger or keyboard logger) is an invisible keylogger for Windows that runs hidden in the background to secretly record keystrokes typed, passwords entered, websites visited, applications/files used and screenshots of activities.

Revealer Keylogger

Source: http://www.logixoft.com

Revealer Keylogger uses an algorithm that can record keystrokes, including passwords, regardless of the application used (e.g., MSN, AOL, ICQ, AIM, GTalk, Skype, Facebook). It allows remote monitoring with report delivery via email, FTP, or LAN.

Spy Keylogger

Source: http://www.spy-key-logger.com

Spy Keylogger is a utility that records all ASCII keystrokes to special log files. It preserves your information from all activities and lets you easily review the saved information and recall forgotten email or a URL. Spy Keylogger supports work in stealth mode, so that you will be the only one who will know the program is running.

Realtime-Spy

Source: http://www.realtime-spy.com

Realtime-Spy can log and record anything users do at the computer, as well as display, *in real time*, what they are doing and typing.

Features:

- Keystrokes and passwords typed
- Websites visited and online searches
- Internet connections made
- Durations of Internet activities
- Screenshots of user activity
- All window interactions

SpyBuddy® 2013

Source: http://www.exploreanywhere.com

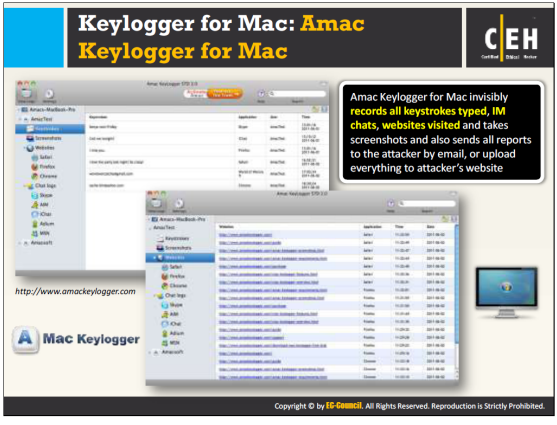
SpyBuddy 2013 is undetectable computer-monitoring software that captures all screens and records users' actions.

Features:

SpyBuddy 2013 records all of the following types of actions and more.

- Keystrokes
- Programs run
- Websites visited
- Files or videos downloaded
- Emails sent or received
- Documents printed

It is remotely accessible from your web browser—anytime and from anywhere—and presents your recorded activity data through flexible, accurate, and easy-to-understand reports.

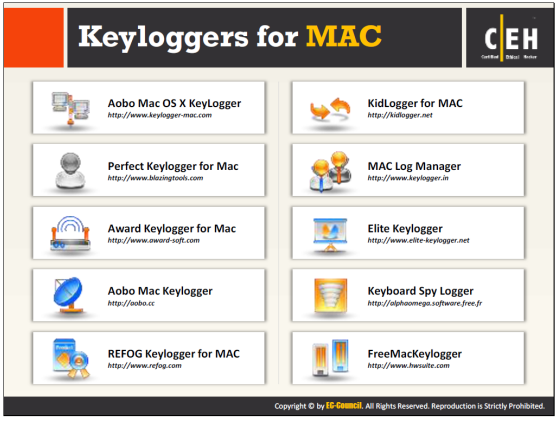


Amac Keylogger for Mac OS X is a Mac application that allows users who want to spy on users of Macintosh computers and secretly record all information, including passwords, keystrokes, chat conversations, websites visited and screenshots captured.

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

Source: http://www.amackeylogger.com



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:

Aobo Mac OS X KeyLogger

Source: http://www.keylogger-mac.com

Aobo Keylogger, is a spy app for Mac that logs keystrokes, passwords, chats, websites, screenshots, IP locations, and more. Running in the background, Aobo Mac Keylogger secretly delivers all the activities on the Mac as logs to you by email or FTP.

Perfect Keylogger for Mac

Source: http://www.blazingtools.com

Perfect Keylogger for Mac OS X offers remote monitoring support. It invisibly records all keystrokes, captures chat in both directions, captures screenshots, records websites visited, and can send the logs back to you by email or FTP.

Award Keylogger for Mac

Source: http://www.award-soft.com

Award Keylogger for Mac records all user activities. One can convert the information into HTML format for suitable viewing on your Web browser and send it secretly through email.

Aobo Mac Keylogger

Source: http://aobo.cc

Aobo Mac Keylogger records all keystrokes on a Mac, regardless of application, and sends the logs to you by email/FTP.

REFOG Keylogger for Mac

Source: http://www.refog.com

Refog Keylogger for Mac records all keystrokes. It also takes screenshots periodically and saves them for your viewing. Additionally, it records outgoing chat messages, website visits, and application usage.

KidLogger for Mac

Source: http://kidlogger.net

KidLogger for MAC is an activity monitoring tool that allows you to monitor activities on Apple mobile devices and Mac computers. It can act as a keystroke logger, and can function as a user activity monitor, web history monitor, and screen capture program. It allows you to monitor several Mac computers at a time easily using a website log viewer.

MAC Log Manager

Source: http://www.keylogger.in

MAC Log Manager records various user activities when using Apple mac machines. It is a monitoring software for Mac records keystroke details, clipboard contents, Internet usage, along with USB drive insertion/removal activities in complete surveillance mode.

Elite Keylogger

Source: http://www.elite-keylogger.net

Elite Keylogger is a keylogger for recording keystrokes. It captures all words typed on websites, emails, chats, and instant messages.

Features:

- Collects social network passwords
- Monitors all websites visited
- Quick and easy installation
- Gets private email reports
- Keeps teens safe online
- Captures emails and screenshots
- Records IM chat history (both directions)

Keyboard Spy Logger

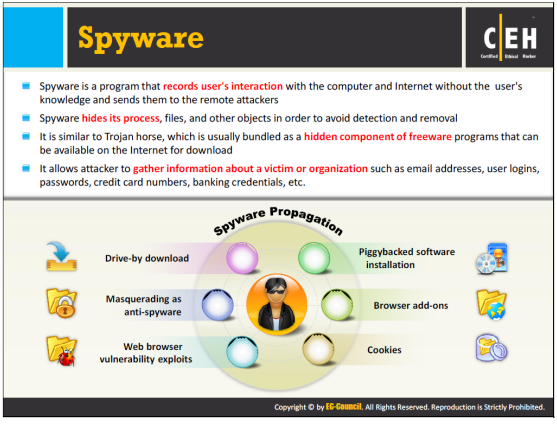
Source: http://alphaomega.software.free.fr

Keyboard Spy allows you to spy on and record in the background all keystrokes in a log file, except passwords protected by Mac OS X itself, and saves application-switching information. It is an invisible background application that does not appear in the Dock.

FreeMacKeylogger

Source: http://www.hwsuite.com

FreeMacKeylogger monitors and logs keystrokes on your Mac, in any language installed on your computer, and tracks applications.



Spyware is stealthy computer monitoring software that allows you to secretly record all the user activities on the target computer. It automatically delivers logs via email or FTP, including all areas of the system such as email sent, websites visited, every keystroke (including login/password of ICQ, MSN, AOL, AIM, and Yahoo Messenger or Webmail), 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 usually bundled as a hidden component of freeware or shareware programs downloaded from the Internet.

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 slow 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 and Internet Spyware

- **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 install it 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.

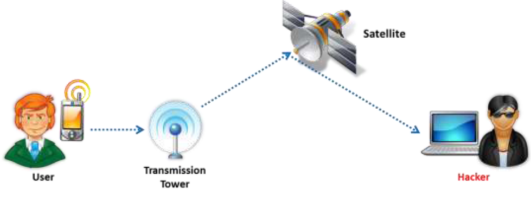


FIGURE 5.6: Telephone/cellphone Spyware

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.

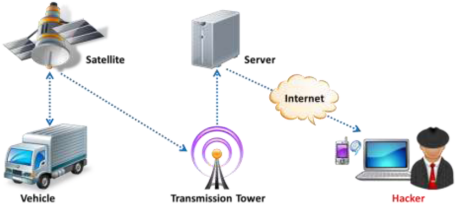


FIGURE 5.7: GPS Spyware

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

Source: http://www.spytech-web.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 with time stamps and user IDs.
- **Email Recording:** Power Spy records all emails read in Microsoft Outlook, Microsoft Outlook Express, WinMail, 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.

Source: *http://ematrixsoft.com*

NetVizor

Source: http://www.netvizor.net

NetVizor comes with an unparalleled task recording feature-set that in secret records everything employees do on your network. Chats, keystrokes and emails, site and online search activity, application usage, file usage, uploads and downloads, computer software setups, and web traffic represent simply a sampling of the NetVizor activity recording capabilities. It records visual proof of all network behavior with the built-in screen capturing and playback.

Remote Desktop Spy

Source: http://www.global-spy-software.com

Remote Desktop Spy is a computer surveillance program for the home, school, or office purposes to monitor and record every detail of PC and Internet activity. The program contains several integrated tools which work together to record all programs used, keystrokes typed, websites visited, files created or changed, and a screenshot logger which can take hundreds of snapshots every hour.

Spector CNE Investigator

Source: http://www.spectorcne.com

Spector CNE Investigator helps you to monitor the computer activity of suspicious employee. Spector CNE Investigator capture screen snapshots, tracks every file and program download over the Internet, captures and stores email from corporate email platforms, and many more.

REFOG Employee Monitor

Source: http://www.refog.com

Refog employee monitoring software allows managers and supervisors to monitor your multiple employee activities and provides you on-site and remote access to employee's logs and computer screens in real time. The software is completely invisible to the employees.

Employee Desktop Live Viewer

Source: http://www.nucleustechnologies.com

The tool helps effectively monitor and record employee activities on a computer network with the help of the Employee Desktop Live Viewer. It tracks online as well as offline activities of individual employee on a system network. It also records employee activities such as web access, download history, chat logs, and others in the AVI video format.

Activity Monitor

Source: http://www.softactivity.com

Activity Monitor is a tool that allows you to track any LAN, giving you the most detailed information on what, how, and when network users are performing on the network. This system consists of server and client parts. The user can install Activity Monitor Server on any computer in the whole LAN. Install Remote spy software on all computers on the network that you want to monitor. Remote spy software, also known as the Agent, is a small client program. You can install the agent can remotely from the PC with Activity Monitor Server on it or via Active Directory Group Policy in Windows domain.

The tool helps to remotely monitor any computer in the network with this tool just by installing the Agent on the computer. You can tune the activity monitor software to record activities of all the computers connected to the network.

Child Control 2014

Source: http://www.salfeld.com

Child Control allows you to control your child's computer usage. It restricts access to Web sites, browsers, messengers, games, programs, files and folders. The program includes the powerful Internet filter which protects your child from an obscene Web content and makes logs of child's unwanted PC activities. An attacker can use this tool as spyware software on the target system.

Net Nanny Home Suite

Source: http://www.netnanny.com

Net Nanny Home Suite allows you to track and monitor what your children are doing on the computer. One can use it as configured right "out of the box" or modify the filter settings according to personal preferences and necessities. It allows you to see logs of children's activities such as usenet, peer-to-peer downloading networks, chat Rooms, FTP, forums, email and instant messages from anywhere through remote management tools.

SoftActivity TS Monitor

Source: http://www.softactivity.com

SoftActivity TS Monitor is a terminal-server session recorder that captures every user action. It allows you to monitor the remote user's activities on your Windows terminal server and monitor your employees who work from home or a remote area and during business trips via RDP. This can also monitor what users do on the client's network, without installing any software on your network. It can document server configuration changes by recording remote and local administrative sessions. Secure your corporate data by preventing information theft by insiders. Increase staff productivity and improve security. This terminal server monitoring software is completely invisible to monitored users.

SPECTOR Pro

Source: http://www.spectorsoft.com

SPECTOR PRO software captures every single Keystroke, including passwords, captures and reviews all chats and instant messages (both sides), reads every email sent and received, including web-based emails, reviews every website they visit, and observes what they do while on them, sees everything they do on Facebook and social networks (including all the profiles they visit and pictures they post). You can remotely review the recordings from another PC or Mac, and block users from visiting any website or chatting with anyone to whom you disallow access.

eBLASTER

Source: http://www.spectorsoft.com

eBLASTER monitors the online activity of children or employees from anywhere in the world: at work, in another room of your home, at an Internet café, on vacation—even if you are thousands of miles away.

SSPro

Source: http://www.gpsoftdev.org

SSPro is a parental control and employee monitoring software for concerned parents and business users. With SSPro's advanced parental control features users can: filter websites based on content, keywords or website address; block instant messages when various content or keywords are encountered; set usage-limits on web browser and instant message use; receive email alerts when various events occur; have logs, snapshots sent offsite via email for remote viewing, and much more.

Imonitor Employee Activity Monitor

Source: http://www.employee-monitoring-software.cc

Imonitor EAM (Employee Activity Monitor) is a comprehensive employee monitoring software for company computer monitoring, employee activity monitoring, content filtering, and employee activity reporting. It is able to record everything your employees do such as recording keystrokes typed and website visited, chats, emails, and screenshots. It monitors and controls

employee workstations remotely in stealth mode, and gives you one-click access to view all the computers on your entire network in real-time from one central location.

Employee Monitoring

Source: http://www.employeemonitoring.net

Designed for large and small companies, universities, libraries, and schools, the Employee Monitoring productivity tool is also ideal for many specialized tasks such as usability testing, scientific studies of PC usage, software training tools, remote network security, and much more.

OsMonitor

Source: http://www.os-monitor.com

OsMonitor is an employee monitoring software and network monitoring software for companies in all size. It tracks computer activities such as screenshot, IM conversation, and websites visited. One can find every detail about employees' PC and Internet usage on server, and prevent them from doing something.

Aobo Filter for PC

Source: http://www.aobo-porn-filter.com

Aobo Filter for PC is a web filter software which can block the adult websites automatically, and filter adult websites, games, and applications to protect children. With this advanced filtering technology, you can completely rely on the PC blocker to keep your family safe from adult content.

SentryPC

Source: http://www.sentrypc.com

SentryPC combines features with essential restriction tools like computer usage scheduling, activity filtering and restriction, and behavior reports to create an all-in-one software solution for concerned parents and employers. SentryPC gives you total control over applications and gaming, website activity, chat messenger usage, and virtually any other activity performed on the PC.

Personal Inspector

Source: http://www.spyarsenal.com

Personal Inspector (keylogger) is an employee internet monitoring software, computer monitoring software, parental control, and surveillance tool that helps to monitor what family members are doing on your computer and tracking their Internet usage. Other possible areas of application for this tool are school and university computer labs and Internet cafés for analyzing computer activity of students/visitors and preventing abuse of software licenses and installation of undesired software.

iProtectYou Pro

Source: http://www.softforyou.com

The iProtectYou Internet filtering and parental control software enables you to fully control your child's online use, thus blocking inappropriate, harmful and dangerous aspects of the Internet. In addition, this program enables businesses to limit and control their employee access to the Internet and to any programs.

Spytech SentryPC

Source: http://www.spytech-web.com

SentryPC combines Spytech's powerful computer monitoring expertise with essential parenting and scheduling tools allowing you to put your mind at ease today. Never again will need to wonder what your child is doing on the computer while you are away, or late at night (e.g., chatting online) while you sleep.

Here are some more spyware programs that can be helpful for attackers to monitor victim computer activity.

Email Spy Pro

Source: http://www.emailspyware.com

Email Spy Pro is an email monitoring software and surveillance tool designed for consumers and businesses. Once installed on monitored computer it sends exact copies of all outgoing SMTP-based emails to your secret email address. While monitored user sends emails by using usual email client software, the tool will invisibly copy all his outgoing emails to your secret email address pre-configured via Email Spy Control Panel.

Ascendant NFM

Source: http://www.ascendant-security.com

Ascendant NFM represents the latest in cutting-edge network file monitoring security software and asset protection. Although requiring absolutely no software installation on any computer on your network, it can centrally monitor and record every single file action that occurs on your network. Every file opening, creation, modification, and deletion is recorded along with the user that performed the action, and when. In addition, Ascendant NFM contains essential logging tools that will log and show you every application and website used by users on your network.

CyberSpy

Source: http://www.cyberspysoftware.com

Cyber Spy is a local computer monitoring software program for your computer monitoring and internet keylogger needs. Record everything your employees, child, spouse, or others do on your PC. With stealth capabilities CyberSpy can not only record all keystrokes typed via built-in keylogger, but also all websites visited, internet chat conversations, documents opened, and so much more.

AceSpy

Source: http://www.acespy.com

AceSpy's Spy Software, also known as monitoring software, is a computer program that secretly monitors your PC's activity. AceSpy completely records chat conversations, emails, websites, Facebook, and other Internet activity. This computer spy program runs in complete stealth, so that it remains completely hidden to others.

SSPro

Source: http://www.gpsoftdev.com

SSPro is a computer monitoring software and keylogger software. It acts as both parental control and employee monitoring software for concerned parents and business users. It is an alternative to emailing activity log files and snapshots, and you can configure SSPro to monitor multiple machines on a network simultaneously.

RecoveryFix Employee Activity Monitor

Source: http://www.recoveryfix.com

RecoveryFix Employee Activity Monitor software is an employee monitoring utility, which is useful for the business owners to keep a track of and monitor all activities of their employees. RecoveryFix Employee Activity Monitor software takes note and displays every activity carried out by the user with the particular computer. It displays the desktop screenshots, visited websites, chat logs, Interned activities, typed keystrokes, downloaded files, opened/closed windows, and much more.

Net Spy Pro

Source: http://www.net-monitoring-software.com

Net Spy Pro is an employee network monitoring software. This program allows you to monitor and control all user activity on your network in real time from your own workstation. The program makes it easy to see what users are doing and whether or not they are wasting time.

LANVisor

Source: http://www.lanvisor.com

Designed for use on the Local Area Network (LAN), the tool helps to monitor and record user activity. The LANVisor system is compatible with remote control software, which allows you to control the mouse and keyboard of a computer connected to the network.

Work Examiner Standard

Source: http://www.workexaminer.com

Work Examiner Standard is a solution for controlling employees' office hours. The software allows organizations to quickly and at the minimum cost monitor and analyze the activity of their employees on the Internet and in various applications.

CyberSieve

Source: http://www.softforyou.com

It is an internet filtering and parental control software, gives you the ability to control and monitor your child's use of the Internet, irrespective of where you are: in the neighboring room, at work, or even on vacation, thus enabling you to protect your child from the dangers of the Internet. In addition, this program enables businesses to limit and control their employee access to the Internet and to any programs.

K9 Web Protection

Source: http://www1.k9webprotection.com

K9 delivers the comprehensive protection you need automatically. With K9, you get the same advanced Web filtering technology used by enterprise and government institutions worldwide—all with a user-friendly interface that allows you to control Internet use in your home. In addition to filtering the categories or sites you choose, K9 also offers real-time malware protection, automatic content ratings, and continuous protection that will not slow down your computer.

Verity Parental Control Software

Source: http://www.nchsoftware.com

Verity parental control software allows you to track and monitor what your children are doing on the computer and online in an easy, non-invasive way. It monitor computer activity both online and off, blocks websites and applications with parental controls, captures screenshots at regular intervals, and track computer usage by user and programs.

Profil Parental Filter

Source: http://www.profiltechnology.com

Profil Parental Filter solution controls your children's access to the Internet with six categories of filtering (pornography, violence, racism, gambling, weapons, and drugs). This solution integrates ICE technology which can detect whether or not a given web page is appropriate for a child. It takes all web content into account, including Web 2.0 content.

PC Pandora

Source: http://www.pcpandora.com

PC Pandora is a monitoring software that records all computer activity. It gives you the ability to view detailed screen captures and text-based data logs of all activity, so you can know everything that happens on the computer. From instant messenger chats to websites visited (and how often and for how long) to programs and applications run, you—the parent—can see everything.

KidsWatch

Source: http://www.kidswatch.com

KidsWatch parental control software safeguards your family's internet experience, blocks dangerous and inappropriate websites, delivers real time alerts and reporting, and sets time

management and controls. It is loaded and preloaded with many optional benefits and features that improve the security and the quality of the Internet your children see.

Desktop Spy

Source: http://www.spyarsenal.com

Desktop Spy Agent is PC monitoring software. It captures the screenshots of the computer desktop and programs launched. These images are stored in a separate folder as BMP or JPEG files and later view them with a built-in viewer or external applications. You can customize the intervals of screen capturing. The program runs invisibly in the background and is extremely difficult to discover.

IcyScreen

Source: http://www.16software.com

IcyScreen is an automatic screenshot taker/automatic screen capture program that can automatically save screenshots to disk, upload them to a web server via FTP, and e-mail them to an unlimited number of recipients, including you.

PC Tattletale

Source: http://www.pctattletale.com

PC Tattletale records every detail of what they do on the computer—their chats, instant messages, emails, the web sites they visit, what they search for, what they do on Facebook and Social Networks, the pictures they post and look at, the programs they run and much more. You get to see not only *what* they do, but the *exact* order in which they do it, step by step.

Computer Screen Spy Monitor

Source: http://www.mysuperspy.com

Computer Spy Monitor is an invisible PC Keylogger which allows you to secretly record all activities of PC users including all keystrokes and screenshots captured. Moreover, it supports remote monitoring through log report delivery via email without any physical need.

PC Screen Spy Monitor

Source: http://ematrixsoft.com

PC Screen Spy Monitor spy software secretly captures your computer screen. It is like an invisible surveillance camera aimed directly at your PC screen. It records a screenshot every *X* seconds (adjustable) in hidden mode. This captures all activity performed on your PC.

Kahlown Screen Spy Monitor

Source: http://www.lesoftrejion.com

Kahlown Screen Spy Monitor is parental control software to secretly capture screenshots or record screen video in hidden mode. It records everything from the computer screen for watcher it later and is completely invisible to users with encryption (screenshots and video) capability.

Guardbay Remote Computer Monitoring Software

Source: http://www.guardbay.com

GuardBay Online Remote PC Monitoring Software to monitor, you can watch your employees or children from anywhere in the world, and from any device capable of web browsing (Your PC, Laptop, iPhone or Android). It allows you to prevent your employees or children from going off-track when they are on computers (playing games, browsing non-work-related sites, chatting) hence increasing their overall productivity.

HT Employee Monitor

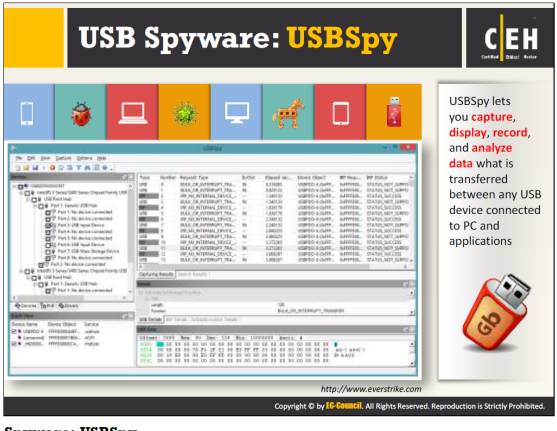
Source: http://www.hidetools.com

HT Employee Monitor records all your employees' computer activities and gives you remote access to this information, including typed keystrokes, visited websites, opened applications, screenshots, and more. The software helps you to increase employee productivity by monitoring, as well as by blocking activities that don't work-related such as Facebook, Twitter, instant messengers, specified web content, and so on.

Spy Employee Monitor

Source: http://www.spysw.com

Spy Employee Monitor is remote monitoring software in LAN to monitor employee computer desktop and activity as a surveillance camera. This LAN spy employee monitoring software monitors the screens of all employees' computers in real time by matrix screen from a single administrator's PC. It will tell you exactly what your employee do in their work time, including recording keystroke, websites visiting, receiving or sending email, MSN chats, and any other activities.



USB Spyware: USBSpy

Source: http://www.everstrike.com

USBSpy lets you capture, display, record, and analyze data transferred between any USB device connected to a PC and applications. This makes it a great tool for debugging software, working on a device driver, or hardware development, and provides a powerful platform for effective coding, testing, and optimization. It makes USB traffic readily accessible for analysis and debugging. Its filters and triggers cut the chase and presents only required data. Its interface makes communications easy to follow.

Features:

- Interception of all I/O requests and events between a USD device and its host
- USBSpy doesn't create any additional filters, devices that could otherwise destroy the structure of drivers in your system
- Extended search and filtering options
- Triggers on packet types, device requests, completion statuses, errors, etc.
- Automatic capture of hot-plugged devices
- Interception at system boot
- Export of traffic logs into XML
- Clear intuitive interface

Here are some more USB spyware programs that can be helpful for attackers to capture, analyze, record, and displays all the data communicated from the device to the host system:

USB Monitor

Source: http://www.hhdsoftware.com

USB Monitor is a used for monitoring and analyzing USB devices and any kind of application working with them on Windows platform. Universal Serial Bus Monitor (USB monitor) allows you to intercept, display, record and analyze USB protocol and all the data transferred between any USB device connected to your PC and applications. It helps in application development, USB device driver or hardware development and offers the powerful platform for effective coding, testing, and optimization.

USBlyzer

Source: http://www.usblyzer.com

USBlyzer is a software-based USB analyzer and USB data traffic sniffer for Windows, which provides a complete yet simple to understand view for monitoring and analyzing USB Host controllers, USB hubs, and USB devices activity.

USBTrace

Source: http://www.sysnucleus.com

USBTrace is a USB analyzer that can analyze USB traffic at host controllers, hubs, and devices.

USBDeview

Source: http://www.nirsoft.net

USBDeview lists all USB devices that currently connected to the computer, as well as all USB devices that previously used. For each USB device, the tool displays extended information: Device name/description, device type, serial number (for mass storage devices), the date/time of device addition, VendorID, ProductID, etc.

Advanced USB Port Monitor

Source: http://www.aggsoft.com

Advanced USB Port Monitor is used to capture, view and process USB traffic. The Advanced USB Port Monitor software allows you to display the packets sent, decode the descriptors, detect errors in peripherals or drivers, and measure device and driver performance.

USB Monitor Pro

Source: http://www.usb-monitor.com

USB Monitor Pro is an analyzer of USB traffic that allows monitoring data streams that go to and from USB devices. You can keep your eye on the process to observe data capturing in real time. It also offers advanced data capturing and displaying filter and can monitor several USB devices simultaneously.

USB Activity Monitoring Software

Source: http://www.datadoctor.org

USB Activity Monitoring Software monitors the USB mass storage device activities on a client's system on Windows network. USB drive activity monitoring software for LAN effectively and efficiently prevent the unauthorized access of USB device activities including insertion and removal of USB devices on clients' machines.

Stealth iBot Computer Spy

Source: http://www.brickhousesecurity.com

The Stealth iBot Computer Spy is a computer monitoring device or software that finds out exactly what people are doing on your computer once installed. The Stealth iBot Computer Spy will record everything typed and viewed on a PC—passwords, chats, emails, and so on—no matter what account a user logs into.

KeyCarbon USB Hardware Keylogger

Source: http://www.spywaredirect.net

KeyCarbon records every keystroke typed on your computer, including email, chat, IM, Internet addresses, and more. The KeyCarbon USB key logger monitors online activities.

USB 2GB Keylogger

Source: http://diji.com

USB 2GB Keylogger (KL2 USB) is an advanced USB hardware keylogger with a 2GB internal flash disk, organized as a file system. Captures all text data typed on the USB keyboard and stores it on the internal Flash Drive in a special file. It retrieved text data on any computer with a USB port and keyboard. It retrieves data switching into Flash Drive mode for keystroke data transmission.

Spy Voice Recorder

Source: http://www.mysuperspy.com

Spy Voice Recorder is a computer spy software that allows you to monitor sound and voice recorder on the system. It invisibly records online chat conversations made in popular chat programs or instant messengers including different types of voice chats available on the Internet such as MSN Voice Chat, Skype Voice Chat, Yahoo! Messenger Voice chat, ICQ Voice Chat, QQ Voice Chat, etc. This can also record other streaming audio from the Internet, music played, sounds from the microphone, earphones, and so on.

Features:

- It records and replays a wider range of sound from microphone, line-in, line-out, streaming audio from the Internet and music played from the computer, even the sound from peripheral equipment.
- The software supports auto recording task trigger options. You can select to auto record when any VoIP software is taking voice conversations.
- Spy Voice Recorder supports to set time length of the recording file. It auto saves new file when the recording time length exceeds to your setting.

Sound Snooper

Source: http://www.sound-snooper.com

Sound Snooper is computer spy software that allows you 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. You can use this in recording conferences, monitoring phone calls, radio broadcasting logs, spying and employee monitoring, and so on. It has voice activated recording, can support multiple sound cards, stores, records of any sound format, sends emails with recorded attachments, and is supported by Windows.

Features:

- **Multiple sound card support:** Sound Snooper supports recording from multiple sound cards simultaneously.
- **Voice activated recording**: The program automatically starts and stops recording (only voice recording).
- **Totally stealth recording:** Nobody can learn that Sound Snooper is active.
- **Supports all possible sound formats:** You can record WAV files in any format—MP3, PCM, GSM, ADPCM, and many others.
- **Low system resources using:** Sound Snooper uses little system resources while recording and even less when it's in standby mode.

Video Spyware: WebCam Recorder

Source: http://webcamrecorder.com

Many video spyware programs are available in the market for secret video surveillance. The 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.

WebCam Recorder is video surveillance software that allows you to record anything on screen such as webcams playing in your browser, video IM conversations, and content from video sites such as YouTube, and video playing on your desktop.

A few of the video spyware programs used for these purposes are listed as follows:

WebcamMagic

Source: http://www.robomagic.com

WebcamMagic records snapshots at regular, specified intervals from the any webcam and automatically download and save images from local or remote in order to view, play back, or process them in various ways.

MyWebcam Broadcaster

Source: http://www.eyespyfx.com

MyWebcam Broadcaster is a service that lets to view their webcam anywhere in the world via both the Internet and mobile phone.

Features:

- Ability to add IP/Network cams
- Archive image snapshots from your camera at regular intervals and make time-lapse animations of your webcam
- Control of Logitech and Creative pan/tilt USB webcams
- Broadcast multiple cameras on one account

Digi-Watcher

Source: http://www.digi-watcher.com

Digi-Watcher is webcam software that monitors your home or office 24 hours a day, captures motion event using webcam, saves into compressed video clips with audio, and triggers various alerts including FTP upload, email, or phone. It also has camera image broadcasting capability, which can publish your webcam on a remote website or Digi-Watcher's embedded web server.

NET Video Spy

Source: http://www.sarbash.com

NET Video Spy is a video-surveillance system that allows you to monitor remote locations using LAN (local area network) or wireless network or Internet. NET Video Spy utilizes the power of your webcam or other video capture device and\or microphone to allow you to create your own video-surveillance system.

Eyeline Video Surveillance Software

Source: http://www.nchsoftware.com

EyeLine Video Surveillance Software helps to monitor home or manage security for a large corporation.

Capturix VideoSpy

Source: http://www.capturix.com

Capturix VideoSpy used to record all video activity with a programmed schedule, insert data in picture, work as a motion detector, record sound, and have event trigger program alerts. It supports any video capture device VFW, WDM, FEB, and WNV.

WebCam Looker

Source: http://felenasoft.com

WebCam Looker is video surveillance software for Windows. It turns your computer into a comprehensive video security system to watch your home or business remotely. One can keep an eye on everything they care of: home, kids, pets, office, cars, and valuables.

SecuritySpy

Source: http://www.bensoftware.com

SecuritySpy will enable to quickly set up an effective video surveillance (CCTV) system. SecuritySpy's motion-detection feature will intelligently detect and capture events, while the remote monitoring feature allows to view cameras over the Internet from anywhere in the world.

iSpy

Source: http://www.ispyconnect.com

iSpy uses cameras, webcams, IP cams, and microphones to detect and record movement or sound. Compresses captured media to flash video or mp4 and streamed securely over the web and local network. iSpy can run on multiple computers simultaneously and has full Email, SMS, and Twitter alerting functions, as well as remote viewing.

1AVMonitor

Source: http://www.pcwinsoft.com

1AVMonitor captures video and audio, broadcast of audio and video, and remote surveillance of audio and video. With 1AVMonitor one can make secure remote surveillance of video and audio from any source of your PC, and be able to view files and real-time content from anywhere.

Mobile Spy is mobile spyware that enables you to monitor and record the activities of a target mobile phone. However, you first need to install this software on the target phone. With the help of this software, you can record activities, logs, and GPS locations of the target. To view the results, you simply need to log in to your secure account using any computer or mobile web browser. Displays logs by categories and sorts them for easy browsing.

It allows an attacker to record text messages, monitor social media, monitor websites, track GPS location, record photos and videos taken, watch the live control panel, view call detail, and so on.

Source: http://www.phonespysoftware.com

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:

VRS Recording System

Source: http://www.nch.com.au

VRS is a digital audio-recording application with robust recording options for easy day-to-day recording. It can record multiple audio channels simultaneously with automatic level control and digital signal processing to improve voice intelligibility.

Modem Spy

Source: http://www.modemspy.com

Modem Spy Software to record phone calls automatically using a voice modem. It can also record audio from the microphone like Dictaphone. An attacker can use the tool as mobile spyware to record the mobile communication of target users without noticing.

MobiStealth Cell Phone Spy

Source: http://www.mobistealth.com

Mobistealth Cell Phone Monitoring Software used to secretly track all cell phone activities of the target user and sends the information back to your Mobistealth user account. It can monitor iPhone, BlackBerry, Android, Nokia, and Windows Mobile phones.

SPYPhone GOLD

Source: http://spyera.com

SPYPhone GOLD is phone software that secretly records all the phone activities such as SMS, call history, emails, phone book, and delivers the recorded information to a web account. This tool also allows to listen to the phone conversation and to know the location of the device.

SpyPhoneTap

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

SpyPhoneTap Software is a cell phone spying software for mobile phone surveillance. This tool makes your monitoring and tracking discreet, completely stealthy, and you could do your monitoring from any part of the world. SpyPhoneTap lets you listen to the conversations and sounds near the phone.

FlexiSPY

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

FlexiSPY is mobile monitoring software that can spy every type of communication, track SMS and GPS locations, browser and application activity. This tool offers call interception and spy calls—letting you listen to phone calls and ambient sounds as they happen.

SpyBubble

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

SpyBubble is a cell phone monitoring and tracking software that can monitor all phone activities 24/7, from SMS Tracking to geo-location tracking. The phone's user will never know.

MOBILE SPY

Source: *http://www.mobile-spy.com*

Mobile Spy is mobile spy software used to record activities, logs and GPS locations and quickly upload it to the Mobile Spy account. It displays Logs by categories and sorts them for easy browsing within a Mobile Spy account.

StealthGenie

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

StealthGenie is the cell phone spy and tracking software that lets you monitor all the activities of any iPhone, Blackberry or Android phone. It starts uploading the monitored phone's usage information and its exact location. You can view it by logging in to your StealthGenie user area from any computer in the world. This state-of-the-art application works in stealth mode and user cannot find it on the monitored phone.

mSpy

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

mSpy is a mobile monitoring application that can log everything from call history, text messages, WhatsApp chats, to keystrokes and emails.

SPYPhone is GPS spyware software that sends the GPS location of a target mobile phone to your web account via Wi-Fi, 3G, GPRS, or SMS. You need to install this software on the mobile phone that you want to track. Spyera Spyphone will use GPS positioning to show the coordinates of the device and its physical location on a map inside your web account. It is even possible to configure the settings for real-time updates, and to display a path of travel between certain times.

You can do following things using this software:

- Listen to phone call conversations
- Read text messages coming to and from the target mobile
- View the call history of the target mobile
- Locate the position of the target
- Access contact lists and the photos taken
- Read chat messages
- Read the Cell ID and Cell Name of the target mobile

Source: http://spyera.com

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:

EasyGPS

Source: http://www.easygps.com

EasyGPS is software that provides a way to upload and download waypoints, routes, and tracks between your Windows computer and your Garmin, Magellan, or Lowrance GPS. EasyGPS lists all of your waypoints on the left side of the screen, and shows a plot of your GPS data on the right. It backs up and organizes your GPS data, print maps, or loads new waypoints onto your GPS for your next hike or geocaching adventure.

FlexiSPY

Source: http://www.flexispy.com

FlexiSPY is mobile monitoring software that can spy every type of communication, track SMS and GPS locations, browser and application activity. This tool offers call interception and spy calls—letting you listen to phone calls and ambient sounds as they happen.

GPS TrackMaker Professional

Source: http://www.trackmaker.com

GPS TrackMaker Professional creates detailed maps from GPS data. The program uses a hardware key or dongle, an electronic plug that works as an unlock password for GTM PRO®. Connect the plug to the USB port, when you execute GPS TrackMaker Professional®. The plug does not interfere with the operation of the printer, scanner, or other devices.

MOBILE SPY

Source: http://www.mobile-spy.com

Mobile Spy acts as GPS spy software. Using the Internet capabilities of the phone, recorded activities, logs, and GPS locations, and are quickly uploaded to your Mobile Spy account.

World-Tracker

Source: http://www.world-tracker.com

World-Tracker provides GPS Car Trackers and commercial vehicle tracking products that enable you to know the precise location of a vehicle on a map any time of the day or night.

ALL-in-ONE Spy

Source: http://www.thespyphone.com

With the GPS location feature of ALL-in-ONE Spy, you can identify the GSM or GPS location of the target phone if the device has installed GPS module. You can then take the given GPS coordinates and map the location on any popular mapping software such as Google Maps. This will enable you to pinpoint the location of the target phone at any given time.

Trackstick

Source: http://www.trackstick.com

The Trackstick Mini records its exact route, stop times, speed, direction, altitude, and other valuable information, which you can download and view on your computer. The integrated temperature recorder ensures to monitor all aspects of its environment. It has a vibration detector, combined with proprietary low-power GPS technology.

MobiStealth Pro

Source: http://www.mobistealth.com

Mobile Phone Spy Software, MobiStealth can act as GPS spyware as it provides both real-time tracking, plus location history for comprehensive location reporting.

mSpy

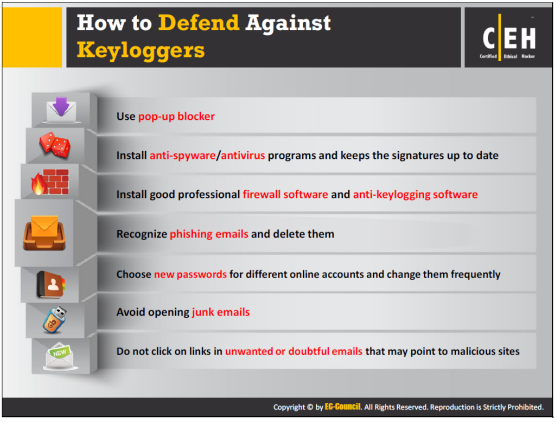
Source: http://www.mspy.com

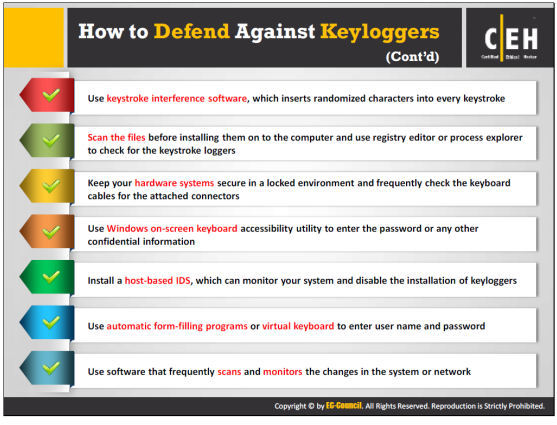
mSpy is a mobile monitoring application that can log everything from call history, text messages, WhatsApp chats, to keystrokes and emails.

TracKing

Source: http://www.spytechs.com

TracKing is a GPS passive tracking system from Spy Chest. It incorporates an ultra-sensitive antenna and power saving impact type sensor is at the core of the TracKing SCI-TK5100. Advanced design and circuitry monitors time, position, and speed at a rate up to once every second of motion, with a horizontal accuracy of approximately 10 feet. The miniature size of this GPS device makes it easy to hide or conceal for covert tracking needs.

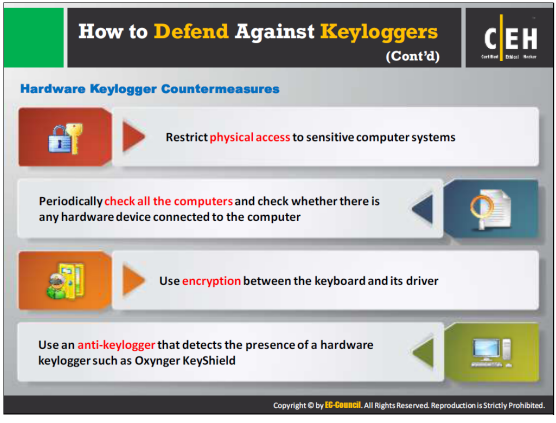




The following are some more ways to defend against keyloggers:

- 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 automatic form-filling programs or a virtual keyboard to enter user names and passwords because they avoid exposure through keyloggers. This automatic form-filling program will remove the use of typing your personal, financial, or confidential details such as credit card numbers and passwords through keyboards.
- Use keystroke interference software, which inserts randomized characters into every keystroke.
- 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.
- 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.
- Update your system software regularly to defend against keyloggers.



- Periodically check your keyboard interface to ensure that no extra components are plugged to the keyboard cable connector.
- Use an on-screen keyboard and click on it by using a mouse.
- Use speech-to-text software to avoid the keyboard connection.
- Use handwriting recognition and mouse gestures that translate cursor movements into the desired text.

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-Keylogger: Zemana AntiLogger

Source: http://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 logger, Screen logger, spyware, SSL banker, Trojans, and so on.

Anti-keyloggers secure your system from spyware, keyloggers. Some of anti-keyloggers help to secure your system against various threats such as:

Anti-Keylogger

Source: *http://www.anti-keyloggers.com*

Anti-keylogger is a dedicated anti-keylogging product. It can protect against even "custom-made" software keyloggers, which are extremely dangerous and very popular with cybercriminals. It runs in the background, quite transparently for the user. It won't ask you needless questions; nor will it distract you from your work. It will guard your privacy and guarantee that all your confidential information remains secret.

PrivacyKeyboard

Source: *http://www.anti-keylogger.com*

PrivacyKeyboard is antispyware software that will help you to protect your PC from spyware and both software and hardware keyloggers. It is better to use PrivacyKeyboard together with anti-virus and firewall to enhance your internet security.

DefenseWall HIPS

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

DefenseWall HIPS (Host Intrusion Prevention System) protects you from malicious software (spyware, botnets, adware, keyloggers, rootkits, etc.) and identifies theft that your anti-virus and anti-spyware programs cannot stop.

KeyScrambler

Source: http://www.qfxsoftware.com

KeyScrambler encrypts your keystrokes in real time to protect your personal information against keylogging in all of the browsers and apps (33 Browsers, 21 Email Clients, 24 IM/VoIP Clients, 2 Music Programs, 36 Online Games, 26 Password Managers, 8 Text Editors, Windows Store [Metro] Apps, 10 Zip Programs, 2 Accounting Programs, 4 Bitcoin Wallets, and many others).

I Hate Keyloggers

Source: http://dewasoft.com

I Hate Keyloggers will prevent the malicious software such as key loggers, spyware, remote administration tools from recording your typing. The software will disable hook-based keyloggers so the keyloggers will not be able to capture your keystrokes. This way you can type sensitive information (passwords, email, credit card number, etc.) with confidence. The log file of the key logger will be empty (your keystrokes are not recorded).

SpyShelter STOP-LOGGER

Source: http://www.spyshelter.com

SpyShelter STOP-LOGGER can help safeguard you against hackers who use a variety of methods to gain your personal information. Whether they try to insert a Trojan virus, hack your webcam, or listen in on your conversations, SpyShelter will protect from the peeping Toms of today's digital world.

GuardedID

Source: http://www.guardedid.com

GuardedID takes a proactive approach to stopping malicious keylogging programs by encrypting every keystroke at the point of typing the keys, and rerouting those encrypted keystrokes directly to your Internet Explorer browser through its own unique path.

PrivacyKeyboard

Source: http://www.privacykeyboard.com

PrivacyKeyboard automatically detects and deactivates all running spy modules on your PC without using any signature bases. It provides protection against windows text capturing, keystroke logging, clipboard capturing, active window screenshot capturing, desktop screenshot snooping, attacks of spy programs, hardware keyloggers, and so on.

Elite Anti Keylogger

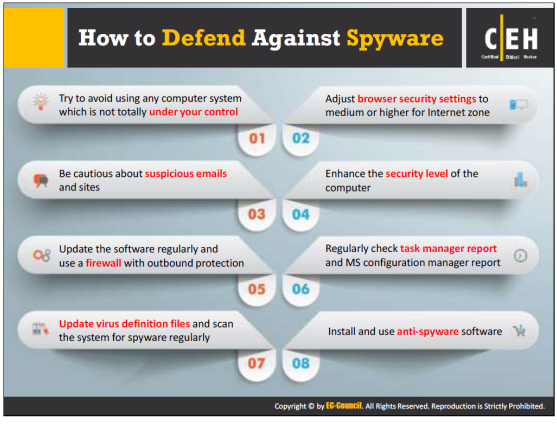
Source: http://www.elite-antikeylogger.com

Elite Anti Keylogger can detect keyloggers and spyware, locate and remove them, protect your PC from unknown attacks and prevent private data loss. Elite Anti Keylogger is simple in use keylogger remover of utmost power. Additionally, it will notify you of any illegal or suspicious behavior of your everyday applications you trust, but might not know about your sensitive information that they are monitoring.

CoDefender

Source: https://www.encassa.com

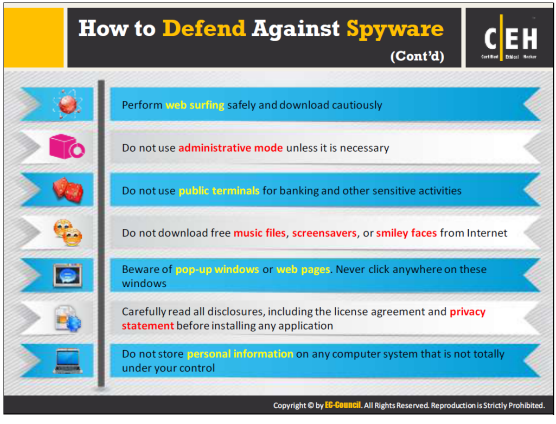
CoDefender computer security software works by encrypting and scrambling your keystrokes at the kernel driver level and decrypting them at the last moment at the protected application level. The tool protects all the vulnerable points of attack from keyloggers, which will record encrypted and scrambled keystrokes that are incomprehensible to the cybercriminal.



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:

- 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.
- 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.
- Enable Firewall to enhance the security level of your computer.
- 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.
- Keep your system up to date.

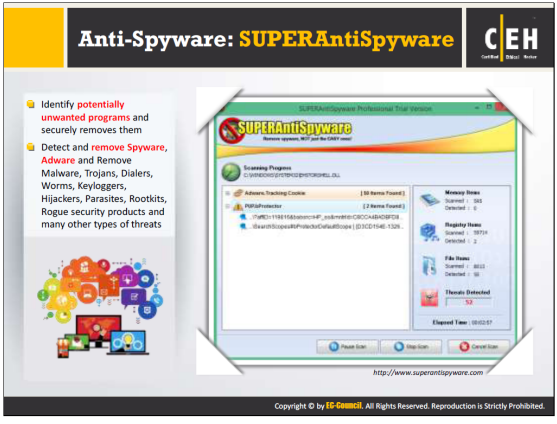
- Windows users should periodically perform the windows update or Microsoft update.
- For other users, using other operation systems or software products, refer to the information given by the operation system vendors, and take essential steps against any vulnerability identified.



Here are some more countermeasures to defend against spyware.

- Perform web surfing safely and download cautiously
  - Before downloading any software, make sure that it is from a trusted website. Read 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 use public terminals for accessing banking account, checking credit card statements, and other sensitive activities. Public systems are not at all secure, as many users can access them. The company that operates the public terminals may not even check their system for spyware.
- 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.



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.

Source: http://www.superantispyware.com

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. Here is the list of some good antispyware programs:

XoftSpySE Anti-Spyware

Source: http://www.paretologic.com

XoftSpySE Anti-Spyware protects your PC from spyware. It scans your computer to find spyware, adware, Trojans, keyloggers, hijackers, pop-up generators and other malware. Once found, XoftSpySE Anti-Spyware powerfully removes these threats.

Spyware Terminator 2012

Source: http://www.pcrx.com

Spyware Terminator 2012 is spyware removal and prevention solution software that prevent you from the risk of losing your privacy and having your computer seriously damaged by spyware. It prevents you from spyware, security breaches and intrusion against your PC.

Ad-Aware Free Antivirus+

Source: http://www.lavasoft.com

Ad-Aware Free Antivirus+ is basically anti-spyware tool that removes spyware from the infected PCs. In addition to antispyware, Ad-Aware Free Antivirus+ is also a powerful antivirus and enhances them with real-time protection, downloads protection and continuously updated filters against malicious URLs, providing top-of-the-line anti-malware protection for the casual computer user.

Norton Internet Security

Source: http://in.norton.com

Norton Internet Security actively protects you from viruses, spam, identity theft and social media dangers. It provides automatic, silent updates that keep you one step ahead of new threats and those not yet invented also.

SpyHunter

Source: http://www.enigmasoftware.com

SpyHunter is a real-time anti-spyware application designed to assist the average computer user in protecting their PC from malicious threats. The automatically configured gives you optimal protection with limited interaction.

Kaspersky Internet Security 2014

Source: http://www.kaspersky.com

Kaspersky Internet Security 2014 combines a vast array of easy-to-use, rigorous web security technologies that protect you against all types of malware and Internet-based threats, including cyber criminals that try to steal your money or your identity. Kaspersky Lab brings you hassle-free security that has minimal impact on your computer's performance.

SecureAnywhere Complete 2012

Source: http://www.webroot.com

SecureAnywhere Complete uses a radically new cloud-based approach to online security that protects you against the latest threats as soon as they emerge. Webroot SecureAnywhere Complete also backs up your files and blocks dangerous web links.

MacScan

Source: http://macscan.securemac.com

With MacScan's Blacklisted Cookie scan, you can remove blacklisted tracking cookies without losing all your saved usernames and passwords. Keep up to date with the latest Spyware definition updates. MacScan searches down these hidden menaces and locks down your computer. MacScan gives you the peace of mind and security needed to conduct your day-to-day personal business.

Spybot – Search & Destroy

Source: http://www.safer-networking.org

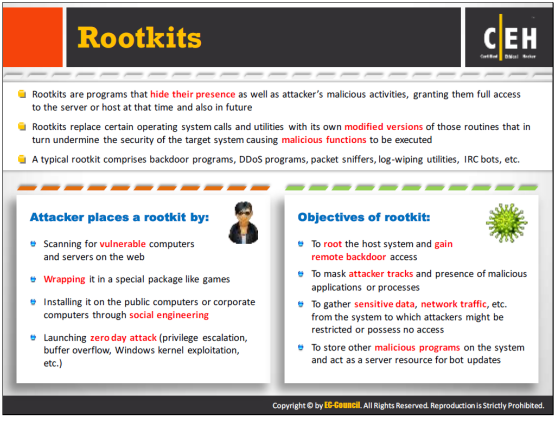
Spybot - Search & Destroy provides anti-virus protection. With a new range of products users can remove annoying startup programs, securely delete files to ensure confidentiality or backup up important registry settings.

Malwarebytes Anti-Malware PRO

Source: http://www.malwarebytes.org

Malwarebytes Anti-Malware Pro detects & removes malware threats and includes anti-spyware, anti-phishing, anti-rootkit, anti-adware, and anti-Trojan, anti-worms, anti-rogues, anti-dialers, and more.

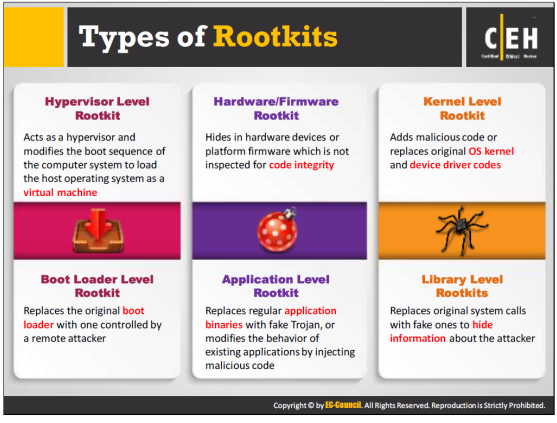
After an attacker has performed malicious operations (i.e., executed malicious applications) on the target system to get escalated access, the next step the attacker will do is to embed and hide his/her malicious programs. The attacker will hide their programs using Rootkits, NTFS Stream, and Steganography 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 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 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 of 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 this 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.



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 hosts 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.

- **Kernel Level Rootkit**

  The kernel is the core of the operating system. These cover backdoors on the computer and created by writing additional code or by substituting portions of kernel code with modified code via device drivers in Windows or loadable kernel module 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.

- **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.

- **Hardware/Firmware Rootkit**

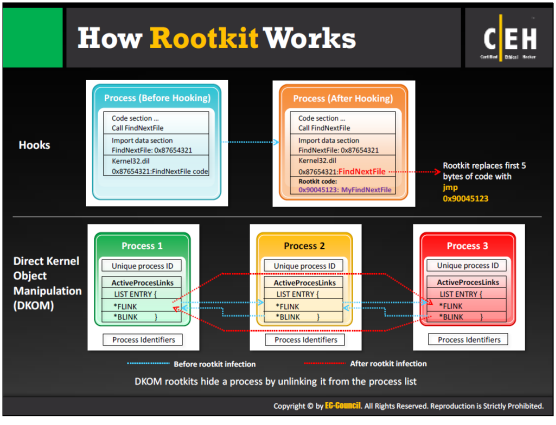
  Hardware/firmware rootkits use devices or platform firmware to create a persistent malware image in hardware, such as a hard drive, system BIOS, or network card. The rootkit hides in firmware as the users do not inspect it for code integrity. A firmware rootkit implies the use of creating a permanent delusion of rootkit malware.

- **Boot Loader Level Rootkit**

  Boot loader level (bootkit) rootkits function either by replacing or modifying the legitimate boot loader 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.

- **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.

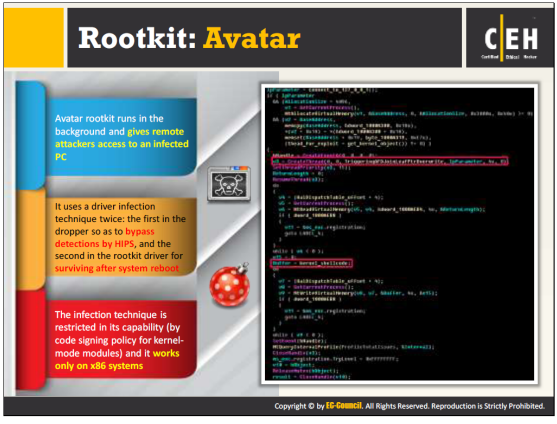


System hooking is a process of changing and replacing the original function pointer with the pointer provided by the rootkit in stealth mode.

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.

DKOM rootkits hide a process by unlinking it from the process list.



Avatar rootkit runs in the background and gives remote attacker access to an infected PC. Avatar rootkit uses a driver infection technique twice: the first in the dropper so as to bypass detections by HIPS, and the second in the rootkit driver for surviving after system reboot. The infection technique is restricted in its capability (by code signing policy for kernel-mode modules), and it works only on x86 systems.

The Avatar rootkit implements a technique for loading the driver by a system driver infection that appeared very effective for bypassing victim's defenses, and allows the loads other kernel-mode modules exploiting the malicious system driver.

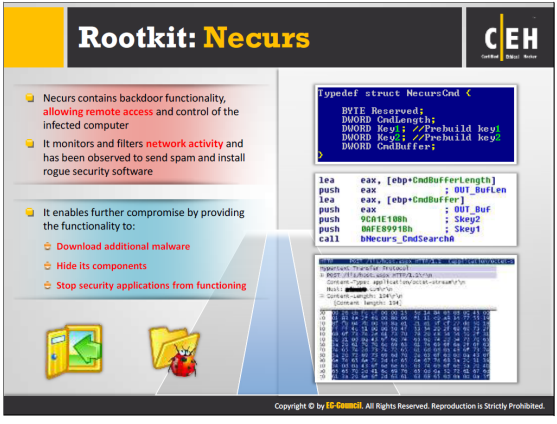
To perform its infection, Avatar randomly chooses a driver and checks its name against a blacklist that varies for every Windows version. The Avatar rootkit driver is able to infect several system drivers without changing the original driver's file size.

The first level dropper implements LZMA decompression for the second level dropper and the malicious driver module.

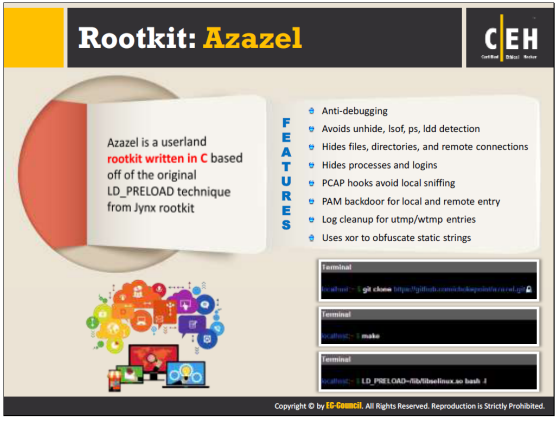
At the next steps the operating system version and current user privilege level are checked. The second level dropper uses two ways of escalating privileges:

1. Exploitation of the MS11-080 vulnerability
2. COM Elevation (UAC whitelist)

The exploit for the MS11-080 vulnerability uses the same exploitation code as a public exploit from the Metasploit Framework with minor changes. After a version check for afd.sys the dropper uses the following exploitation code:



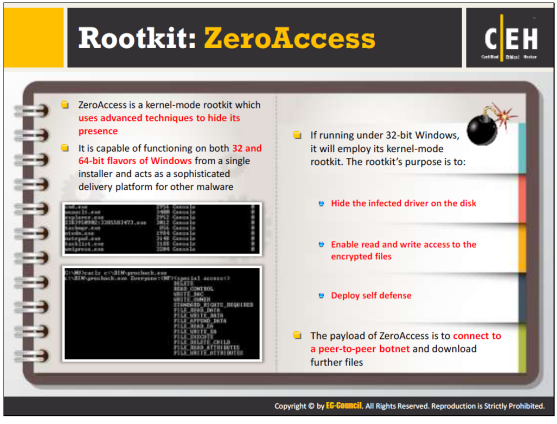
Necurs mostly spreads by drive-by download. The system installs Necurs when someone visits websites compromised by exploit kits such as Blackhole.



Azazel is a userland rootkit written in C based off of the original LD_PRELOAD technique from Jynx rootkit. It is more robust and has additional features, and focuses heavily around anti-debugging and anti-detection.

Features:

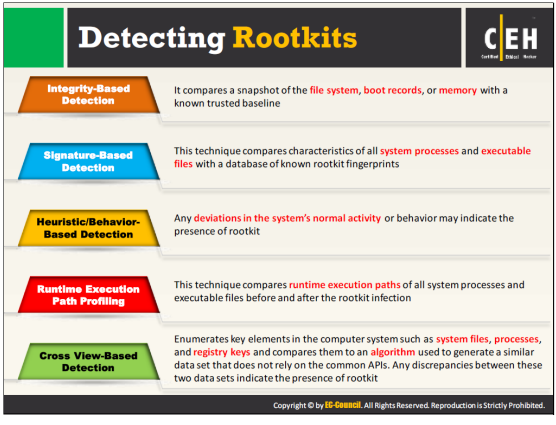
- Anti-debugging
- Avoids unhide, lsof, ps, ldd detection
- Hides files and directories
- Hides remote connections
- Hides processes
- Hides logins
- PCAP hooks avoid local sniffing
- Two accept backdoors with full PTY shells
- Crypthook encrypted accept() backdoor
- Plaintext accept() backdoor
- PAM backdoor for local and remote entry



The main purpose of ZeroAccess rootkit is to gain full control of the machine by adding it to the ZeroAccess botnet and to monetize the new asset by downloading additional malware. Primarily, ZeroAccess is a kernel-mode rootkit. It uses advanced techniques to hide its presence, is capable of functioning on both 32- and 64-bit flavors of Windows from a single installer, contains aggressive self-defense functionality, and acts as a sophisticated delivery platform for other malware.

Attackers distribute ZeroAccess rootkits using following distribution methods:

- **Exploit Packs**: ZeroAccess rootkits is most popular payload for the various Exploit Packs such as Blackhole.
- **Social Engineering**: Convincing a victim into running an executable that they should not do so.



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 attacker 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. 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**

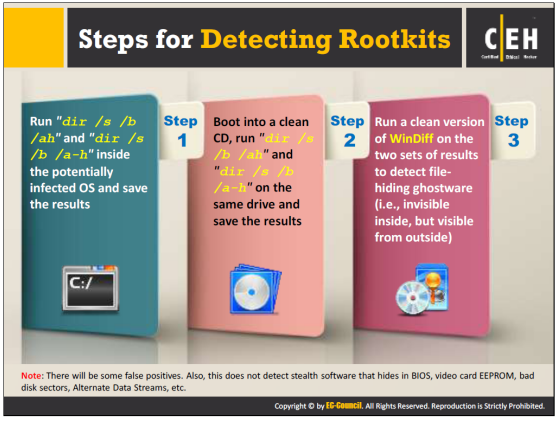
  Heuristic detection works by identifying deviations in normal operating system patterns or behaviors. This kind of detection is also known as behavioral detection. Heuristic detection is capable of identifying new, previously unidentified rootkits. This ability lies in being able to recognize deviants 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 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.



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 finds the way 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.

Refer the slide for steps to detect rootkits by examining file system.

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.

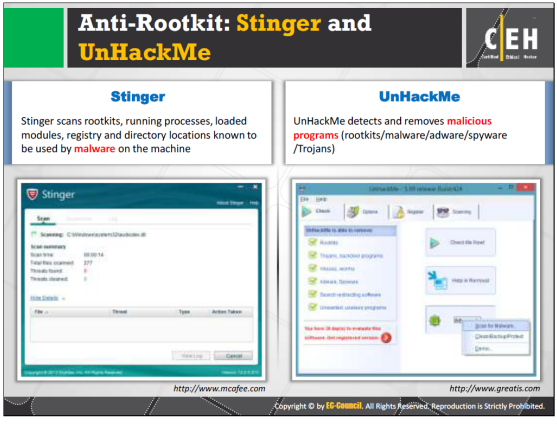
Source: *http://searchenterprisedesktop.techtarget.com*

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:

- Install a firewall and check frequent updates.
- Keep the signatures of anti-malware up to date.
- 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.



The following tools can be useful in preventing rootkit infection on your system:

Stinger

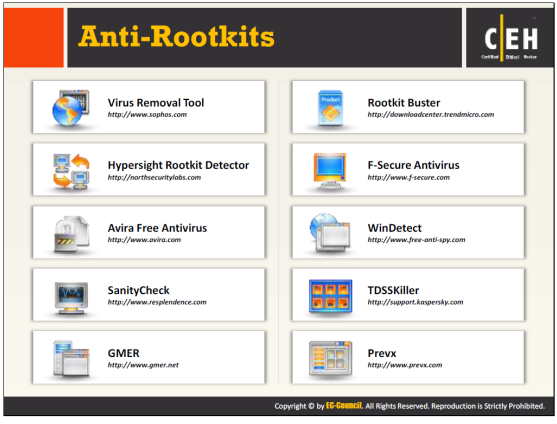
Source: *http://www.mcafee.com*

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.

UnHackMe

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

UnHackMe is basically anti-rootkit software that helps you in identifying and removing all types of malicious software such as rootkits, Trojans, worms, viruses, and so on. The main purpose of UnHackMe is to prevent rootkits from harming your computer, helping users protect themselves against masked intrusion and data theft. UnHackMe also includes the Reanimator feature, which you can use to perform a full spyware check.



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. A few anti-rootkits are:

Virus Removal Tool

Source: http://www.sophos.com

Virus Removal Tool detects all types of malicious software on your computer, including viruses, spyware, and rootkits and returns it to a working state. The tool has ability to detect and remove the very latest viruses.

Hypersight Rootkit Detector

Source: http://northsecuritylabs.com

Hypersight Rootkit Detector is the first Virtual Intrusion Prevention System (VIPS) to use the brand-new approach to detect malicious software. The new approach encapsulates the operating system into a virtual machine, passing control over all critical events to the VIPS core.

The VIPS approach allows detecting the most sophisticated threats and brings your computer security to the new level. Hypersight Rootkit Detector is highly recommended to anyone sharing their financial detail (e.g., credit card numbers) over the Internet, as well as to those demanding the ultimate security.

Avira Free Antivirus

Source: http://www.avira.com

Avira Free Antivirus is basic virus scanners. With pushbutton convenience, this free program removes viruses and other malware. It has ability to block advertising companies from tracking you online.

SanityCheck

Source: http://www.resplendence.com

SanityCheck is an advanced rootkit and malware detection tool which thoroughly scans the system for threats and irregularities which indicate malware or rootkit behavior. By making use of special deep inventory techniques, this program detects hidden and spoofed processes, hidden threads, hidden drivers and a large number of hooks and hacks which are typically the work of rootkits and malware.

GMER

Source: http://www.gmer.net

GMER is an application that detects and removes rootkits. It scans for hidden processes, hidden threads, hidden modules, hidden services, hidden files, hidden disk sectors (MBR), hidden Alternate Data Streams, hidden registry keys, drivers hooking SSDT, drivers hooking IDT, drivers hooking IRP calls, inline hooks.

Rootkit Buster

Source: http://downloadcenter.trendmicro.com

RootkitBuster scans hidden files, registry entries, processes, drivers, services, ports, and the master boot record (MBR) to identify and remove rootkits.

F-Secure Antivirus

Source: http://www.f-secure.com

F-Secure Anti-Virus provides real-time protection against viruses, spyware, infected email attachments and other malware. Automatic updates and advanced real-time response guarantee the fastest protection against all new threats.

WinDetect

Source: http://www.free-anti-spy.com

WinDetect tool removes spyware, adware, Trojan horses, key-loggers, rootkits, and backdoors on your computer. WinDetect product recognizes malicious software by watching for suspicious behavior, not by searching for known offenders.

TDSSKiller

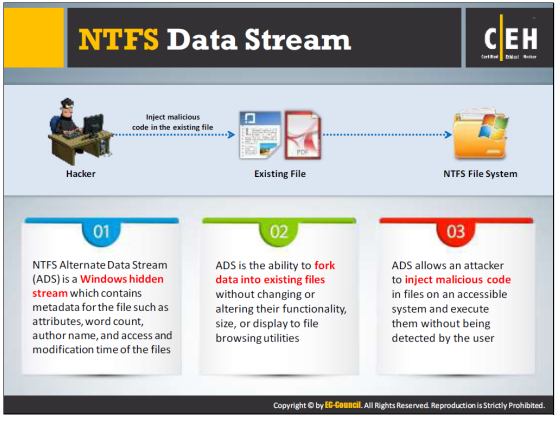
Source: http://support.kaspersky.com

TDSSKiller is a utility that provides the user a simple means of disinfecting any system that suffers from an infection from the rootkits. It helps to detect and remove rootkits from your system.

Prevx

Source: http://www.prevx.com

Prevx CSI is a rapid malware scanner that will find and fix active rootkit, spyware, Trojan, virus, and all other forms of malware infection. It performs fast effective scanning and real-time checking against the most comprehensive malware database in the world.



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.

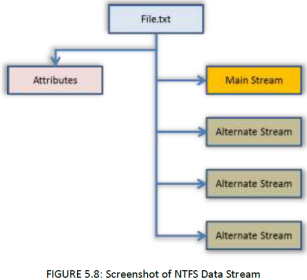


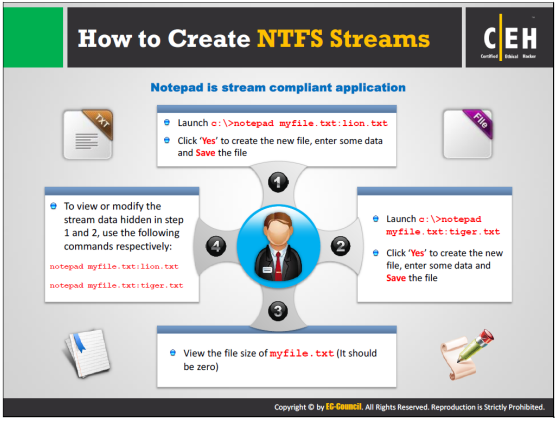
FIGURE 5.8: Screenshot of NTFS Data Stream

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. 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.



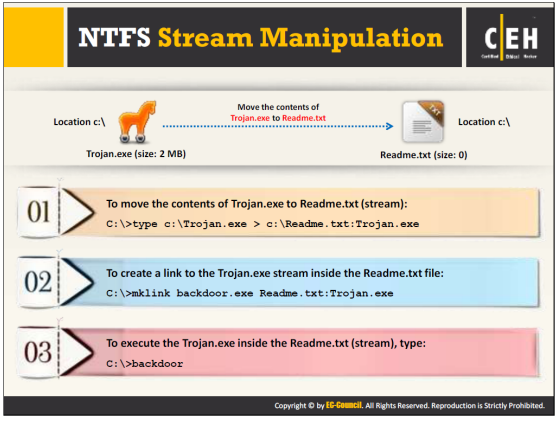
Using NTFS data steam, an attacker can almost completely hide files within the system. It is easy to use the streams but user can only identify it with specific software. Explorer can display only the root files, it cannot view the streams linked to the root files and cannot define the disk space used 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 the file. Alternate data streams follow the syntax: "filename.ext:alternateName"

Refer the slide for steps to create NTFS Streams.

Note: You should not use alternate streams for storing any critical information.



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. 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.

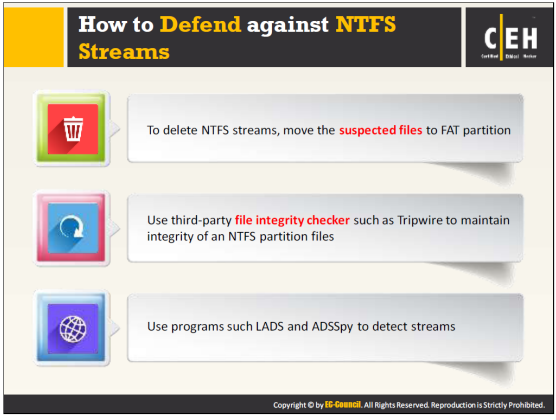
- **Creating a link to the Trojan.exe stream inside the Readme.txt file:**

  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.



You should use Lads.exe 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.

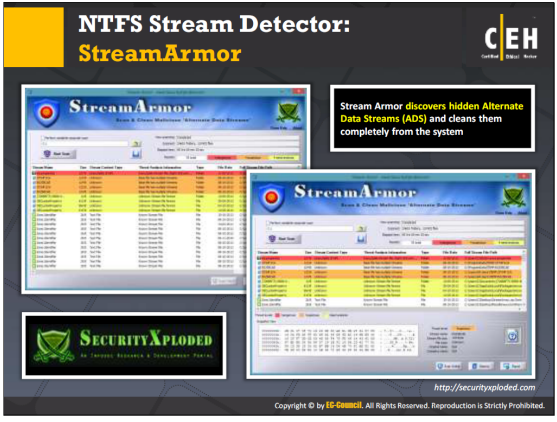
Other means include copying the cover file to a FAT partition, and then moving it back to the NTFS. Where FAT file systems do not support Alternate Data Streams, this will effectively remove them from the original file.

LNS.exe (http://ntsecurity.nu/toolbox/lns/) is another tool used to detect NTFS streams. This tool is useful in forensic investigation.

You should do the following to defend against NTFS streams:

- To delete hidden NTFS streams, move the suspected files to FAT partition.
- Use third-party file checksum application to maintain integrity of an NTFS partition against unauthorized ADS.
- Use third-party utilities to show and manipulate hidden streams such as EventSentry or adslist.exe.
- Avoid writing important or critical data to alternate data streams.
- Use up-to-date anti-virus software on your system.

- Enable real-time anti-virus scanning to protect against execution of malicious streams in your system.
- Use file-monitoring software such as LADS (http://www.heysoft.de) to help detect creation of additional or new data streams.



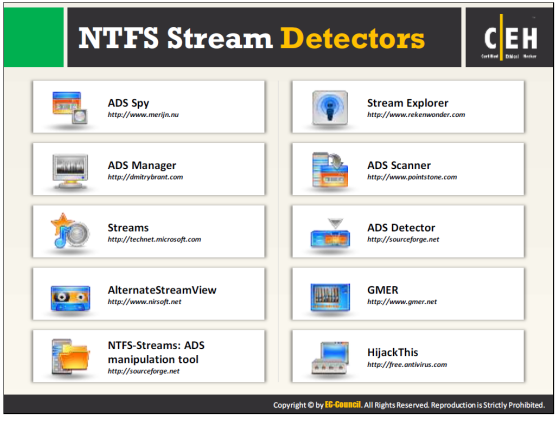
Stream Armor is a tool used to discover hidden Alternate Data Streams (ADS) and clean them completely from your system. Its advanced auto analysis, coupled with an online threat verification mechanism, helps you eradicate any ADSs.

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 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 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.

Source: http://securityxploded.com



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.

ADS Spy

Source: http://www.merijn.nu

ADS Spy is used to list, view, or delete Alternate Data Streams (ADS) on Windows 2000/XP with NTFS file systems. ADS are a way of storing meta-information about files—without actually storing the information in the file it belongs to—carried over from early Mac OS compatibility from Windows NT4. This meta-information is not visible in Windows Explorer.

ADS Manager

Source: http://dmitrybrant.com

Alternate Data Stream Manager (ADS Manager) is a utility for accessing and modifying ADSs within any given file. This is a little-known feature of the NTFS file system that allows one file to contain more than one stream of data, in turn allowing your files to contain "hidden" data that will be invisible to other applications.

Streams

Source: http://technet.microsoft.com

Streams will examine the files and directories (which can themselves also contain ADSs) you specify, and inform you of the name and size of any named stream it encounters in those files. Streams make use of an undocumented native function for retrieving file stream information.

Usage: `streams [-s] [-d] <file or directory>`

`-s Recurse subdirectories.`

`-d Delete streams.`

`Streams takes wildcards e.g. 'streams *.txt'.`

AlternateStreamView

Source: http://www.nirsoft.net

AlternateStreamView is a utility that allows you to scan your NTFS drive and find all hidden alternate streams stored in the file system. After scanning and finding the alternate streams, you can extract these streams into the specified folder, delete unwanted streams, or save the streams list in a text/html/csv/xml file.

NTFS-Streams: ADS manipulation tool

Source: http://sourceforge.net

NTFS-Streams: ADS discovers hidden files never before seen. It is a forensic and security utility to reveal, list, delete, determine contents, extract and copy hidden files from NTFS ADSs.

Stream Explorer

Source: http://www.rekenwonder.com

Stream Explorer will show you the number of streams in each file, as per the list in the folder. When you select a directory entry, Stream Explorer lists all the streams in that entry, and you can see their type, size, and contents. System shows the unnamed stream as <default>.

ADS Scanner

Source: http://www.pointstone.com

Alternate Data Streams (ADS) are pieces of info hidden as file metadata on NTFS drives. They are not visible in Explorer and Windows does not report their size. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Scanner to find and remove these streams.

ADS Detector

Source: http://sourceforge.net

It is an explorer bar that extends the windows explorer functionality and allows viewing Alternative Data Streams on an NTFS drive.

GMER

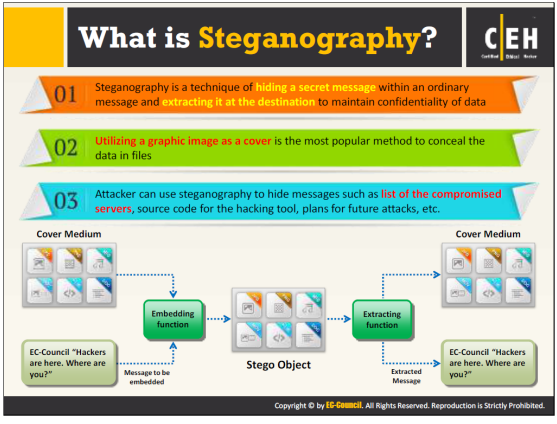
Source: http://www.gmer.net

GMER is an application that detects and removes rootkits. It scans for hidden processes, threads, modules, services, files, disk sectors (MBR), ADSs, and registry keys; drivers hooking SSDT, IDT, and IRP calls; and inline hooks.

HijackThis

Source: http://free.antivirus.com

HijackThis lists the contents of key areas of the Registry and hard drive areas used by both legitimate programmers and hijackers. The developer updates the program continuously to detect and remove new hijacks. It does not target specific programs and URLs—only the methods used by hijackers to force you onto their sites.

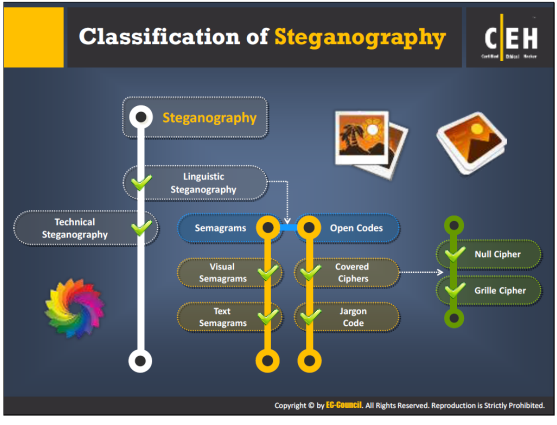


One of the shortcomings of various detection programs is their primary focus on streaming text data. What if an attacker bypasses normal surveillance techniques and still steals or transmits sensitive data? In a typical situation, after an attacker manages to get inside a firm as a temporary or contract 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—graphic, sound, text, audio, video—with some other surreptitiously bits. The hidden data can be plaintext or cipher text, or it can be an image. 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 hacking tool, list of compromised servers, plans for future attacks, communication and coordination channel



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 message existence. It is almost difficult to categorize all these 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 into 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 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 semagrams 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**

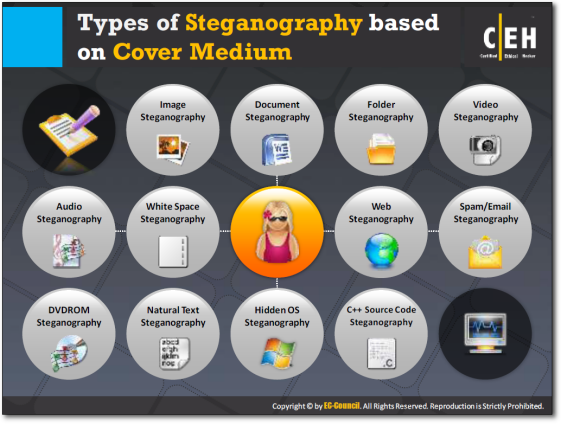
  In this type of steganography, a certain language is used that can be understood by a particular group of people for whom it is addressed, while being meaningless to others. A jargon message is like a substitution cipher in many respects, but instead of replacing individual letters, the words themselves 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.

The diagram in the slide depicts the classification of steganography.



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 is 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, user adds white spaces and tabs in the end of the lines.

- **Folder Steganography**

  Folder Steganography refers to hiding one or more files in a folder. In this process, user moves the file is physically but still keeps associated to its original folder for recovery.

- **Video Steganography**

  Video steganography is a technique to hide any kind of files in 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, user embeds the hidden messages in digital sound format.

- **Whitespace Steganography**

  In the white space steganography, user hides the messages in ASCII text by adding white spaces to the end of the lines.

- **Web Steganography**

  In the 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.

- **DVDROM Steganography**

  In the DVDROM steganography, user embeds the content in audio and graphical.

- **Natural Text Steganography**

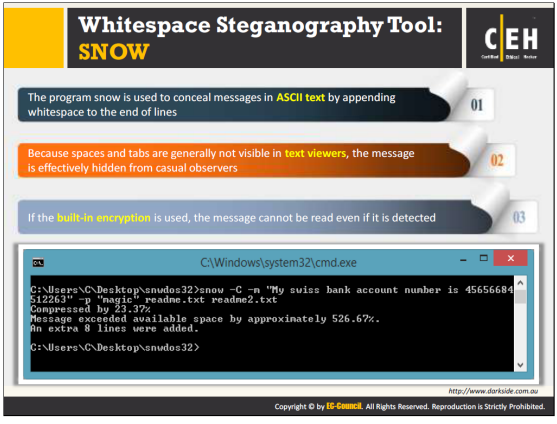
  Natural text steganography is converting the sensitive information into a user-definable free speech such as a play.

- **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.



Snow is a program for concealing messages in text files by appending tabs and spaces on 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.

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. An alternative encoding scheme, using alternating spaces and tabs to represent zeros and ones, users rejected it because it uses fewer bytes but requires more columns per bit (4.5 vs. 2.67).

An appended tab character is 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.

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

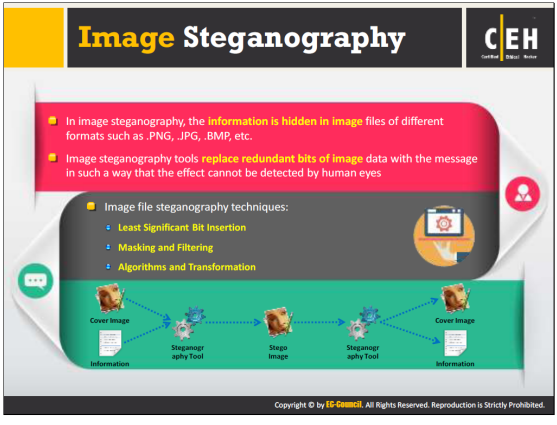
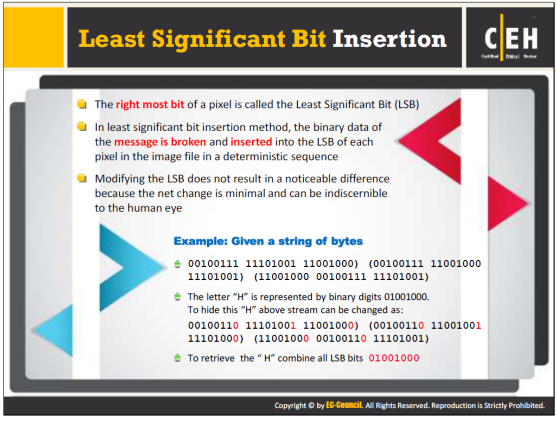


Image steganography allows you to conceal your secret message within an image. You can take advantage of the redundant bit of the image to conceal your message within it. These redundant bits are those bits of the image that have very little effect on the image, if altered. Detection of this alteration 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 ***transform domain*** (frequency) techniques, first, the transformation of images occurs; then the user embeds the message in the image.

Refer to the slide showing image-file steganography techniques and the figure that depicts image steganography and the role of steganography tools in the process.



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. 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:

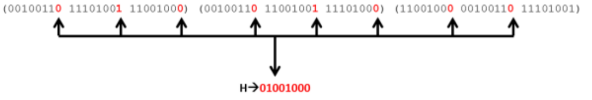
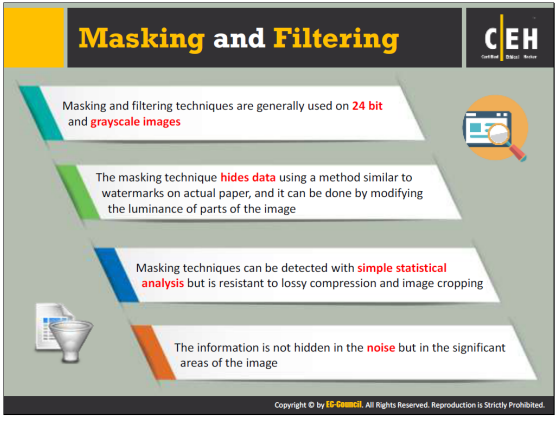


FIGURE 5.9: Example of Least Significant Bit Insertion

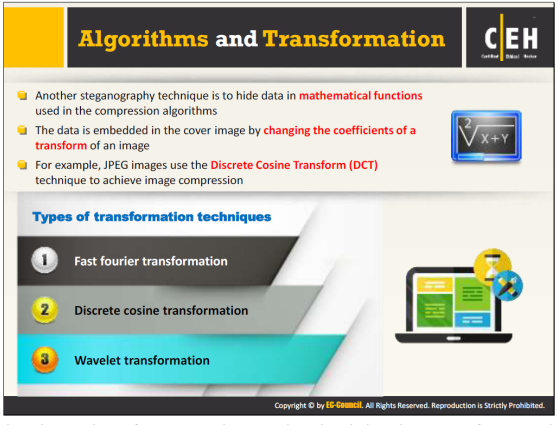
You just need to replace the LSB of each pixel of the image file as shown in this figure.

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 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.



The algorithms and transformation technique is based on hiding the secret information during image compression. In this technique, 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. 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.

QuickStego lets you hide secret messages in images so that only other users of QuickStego can retrieve and read them. Once you hide a secret message in an image, you can still save it as picture file; it will load just like any other image and appear just as before. The user can save, email, upload the image to the web, and the only difference will be that it contains hidden message.

Features:

- Conceals information in folders, images, and sounds
- Keeps all online and offline passwords safe
- Recovers deleted files on NTFS and FAT systems
- Prevents recovery of sensitive files (even already deleted)
- Removes temporary & audit files
- Views and shreds internet browser tracing files
- Tests passwords and attempt password recovery
- Monitors system for potential security flaws

Source: http://quickcrypto.com

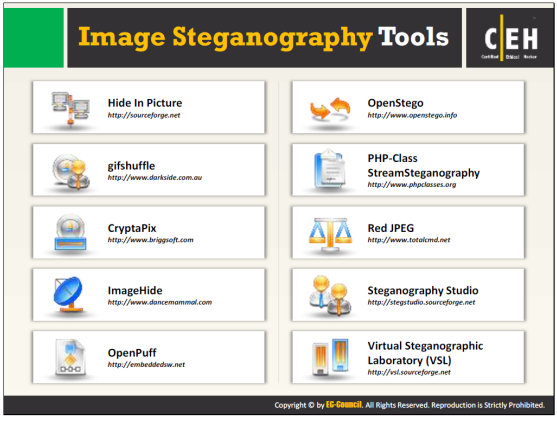


Image steganography tools detect the hidden content in images. You can insert the hidden data into the redundant bits of data sources. You can use image files such as JPEG, GIF, BMP, and PNG to conceal the data.

As with QuickStego (discussed earlier), you can use the following image steganography tools to hide your secret messages in images:

Hide In Picture

Source: http://sourceforge.net

Hide In Picture is a program that allows you to conceal files inside bitmap pictures, using a password. The pictures look like normal images, so people will not suspect there is hidden data in them.

gifshuffle

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

The gifshuffle utility helps to conceal messages in GIF images by shuffling the color map, which leaves the image visibly unchanged. gifshuffle works with all GIF images, including those with transparency and animation, and in addition provides compression and encryption of the concealed message.

CryptaPix

Source: http://www.briggsoft.com

CryptaPix is an image file management and encryption program for windows. Organize, print and secure the digital photos and downloaded image files. Secure proprietary images from unauthorized access with 256-bit AES encryption or hide sensitive text, data, or other images into an image with the secure steganography feature.

ImageHide

Source: http://www.dancemammal.com

ImageHide is an application that lets you hide text messages in images, so you can safely share them with others.

OpenPuff

Source: http://embeddedsw.net

OpenPuff allows users to hide data in more than a single carrier file. It supports image formats such as Images BMP, JPG, PNG, TGA as carrier signals. The sender creates a hidden stream inside some publicly available carrier files. The receiver then extracts the hidden stream using the secret key.

OpenStego

Source: http://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

PHP-Class StreamSteganography

Source: http://www.phpclasses.org

PHP-Class StreamSteganography allows to store hidden and retrieves hidden information from PNG images. It can take a given PNG image and store hidden information in it by using the least significant bits of the color of the image pixels to store encoded information. The class may also do the opposite (i.e., open a PNG image and retrieve previously stored information using the method above).

Red JPEG

Source: http://www.totalcmd.net

Red JPEG is a plug-in for steganographic hiding arbitrary data in JPEG images using unique authors' method. The solution includes open cryptographic algorithms (AMPRNG rev.1.1, Cartman Cipher 2.DDP.4) and effective LZMA compression. The image changes itself slightly, without any visible distortion. Modification practically does not distinguish visually, without having original. Data is user-defined password protected, which is pre-hashed.

Steganography Studio

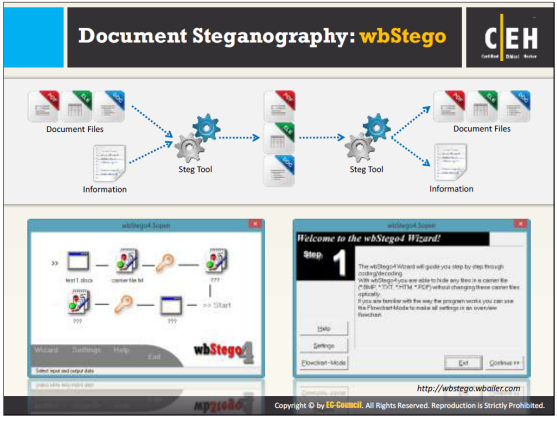
Source: http://stegstudio.sourceforge.net

Steganography Studio is a tool to use and analyze key steganographic algorithms. It implements several algorithms highly configurable with a variety of filters, as well as the best image analysis algorithms for the detection of hidden information.

Virtual Steganographic Laboratory (VSL)

Source: http://vsl.sourceforge.net

Virtual Steganographic Laboratory (VSL) helps in image steganography and steganalysis. The aim of the VSL is hiding data in digital images, detecting its presence and testing its robustness using any number of different adjustable techniques.



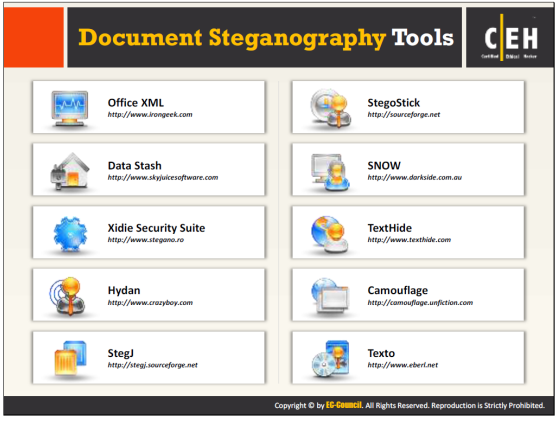
As with image steganography, ***document*** steganography is the technique of hiding secret messages transferred in the form of documents. It includes addition white spaces and tabs at the end of the lines. Stego-document is a cover document comprising hidden message. Steganography algorithms, referred 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 shown in the slide illustrates the document steganography process

wbStego

Source: *http://wbstego.wbailer.com*

WbStego is a document steganography tool. Using this tool, you can hide any type of file within carrier file types such as Windows bitmaps with 16, 256, or 16.7M colors, ASCII or ANSI text files, HTML fields, and Adobe PDF files.



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

Following is the list of some tools that allow you to hide data within other document files:

Office XML

Source: http://www.irongeek.com

Office XML is a program used to hide files inside of Microsoft Office 2007 docs (DOCX, XLSX, PPTX, etc.). The app will create a stego file in the same directory as your cover file, with the prefix "stego". To get back the embedded file just opens the Office document in 7zip.

Data Stash

Source: http://www.skyjuicesoftware.com

Data Stash is a steganographic security tool. It allows you to hide sensitive data files within other files such as large bitmap or database file using steganography. It is useful when you wish to keep out certain files from prying eyes, under the disguise of a normal file.

Xidie Security Suite

Source: http://www.stegano.ro

Xidie security suite is one of the steganography and encryption tools that include facility like: compressed archives (including Zip format), encryption, steganography with 40 carrier types,

secure file deletion, and other components that help to protect computer files and folders and safely store them.

Hydan

Source: http://www.crazyboy.com

Hydan steganographically conceals a message into an application. It exploits redundancy in the i386 instruction set by defining sets of functionally equivalent instructions. It then encodes information in machine code by using the appropriate instructions from each set.

StegJ

Source: http://stegj.sourceforge.net

StegJ Project is a steganography software for academic purpose. It is a cross-platform steganography software written completely in Java, with AES support. The project is extensible, so new steganography algorithms are fully implementable.

StegoStick

Source: http://sourceforge.net

StegoStick allows users to hide any file into any file. It relays on Image, Audio, Video Steganography that hides any file or message into an image (BMP, JPG, GIF), Audio/Video (MPG, WAV, etc.), or any other file format (PDF, EXE, CHM, etc.).

SNOW

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

The SNOW program helps to conceal messages in ASCII text by appending white space to the end of lines. Because spaces and tabs are generally not visible in text viewers, one can effectively hide the message from casual observers. Moreover, if the built-in encryption is used, the receiver cannot read the message if it is detected.

TextHide

Source: http://www.texthide.com

TextHide hides arbitrary data in texts through automatic text rephrasing. It is a secure and inconspicuous method for transmitting and storing information. Various encryption methods are used and additionally it hides the encrypted information so that goes unrecognized.

Camouflage

Source: http://camouflage.unfiction.com

Camouflage allows you to hide files by scrambling them and then attaching them to the file of your choice. With the help of this tool, you can hide a file inside a Word document that will not attract attention if discovered.

Texto

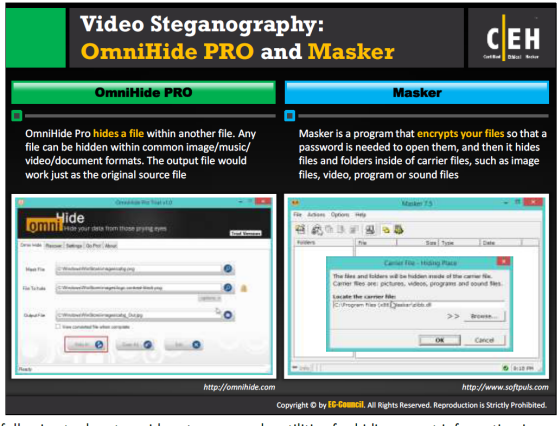
Source: http://www.eberl.net

Texto is an online steganography text steganography program that transforms unencoded or PGP ASCII-armored ASCII data into English sentences.

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 need of hiding large amounts of data inside carrier files.

Video steganography involves hiding secret files of any extensions in a continuously flowing video file. 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. 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.



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

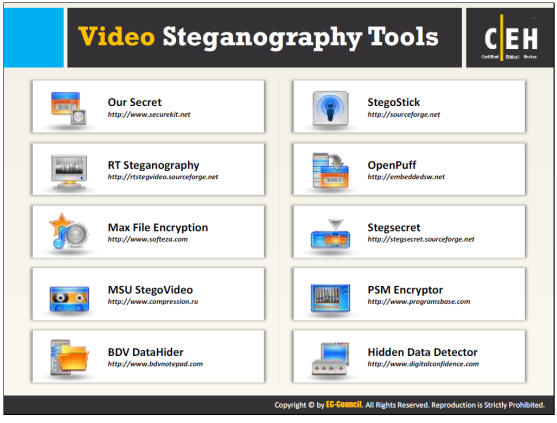
Masker

Source: http://www.softpuls.com

Masker is a program that encrypts files so that it requires a password to open them, and then hides files, folders, and subfolders inside carrier files such as images, video, application, or sound files. Its strong encryption (up to 448-bit) and password protection make the hidden data inaccessible to unauthorized users.

Features:

- Unhides and extracts hidden files and folders from a carrier file
- Offers seven strong encryption algorithms available (BLOWFISH, RIJNDAEL, etc.)



In addition to above discussed video steganography tools, there are many other tools you can use to hide secret data in video files:

Our Secret

Source: http://www.securekit.net

Our Secret enables to hide and encrypt files within other files called carrier files such as image files, video, program or sound files. It hides and sends your sensitive files or messages. It also allows you to encrypt sensitive information, while at the same time hiding it in a file that will not look suspicious.

RT Steganography

Source: http://rtstegvideo.sourceforge.net

Real Time Steganography helps in sending any hidden data, such as text or binary, inside the video files while are streamed to another side.

Max File Encryption

Source: http://www.softeza.com

Max File Encryption is encryption and steganography software that will help to protect confidential information. With Max File Encryption, one can encrypt files of any type (including Microsoft Word, Excel, and PowerPoint documents), hide files inside digital images, audio and video files, and create self-decrypting packages. The program uses the strong and ultra-secure blowfish encryption algorithm that ensures data safety.

MSU StegoVideo

Source: http://www.compression.ru

MSU StegoVideo allows hiding any file in a video sequence. The developers analyzed different popular codecs and chose an algorithm that provides the smallest data loss after compression.

BDV DataHider

Source: http://www.bdvnotepad.com

BDV DataHider is encryption software that will encrypt data with the strongest encryption algorithms known, and then makes it invisible.

BDV DataHider encrypts information and hides it on any drive or in any file: in a picture, in a word document, in a program, in a movie file, and so on. Therefore, it is impossible to discover hidden information in the usual ways.

StegoStick

Source: http://sourceforge.net

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

OpenPuff

Source: http://embeddedsw.net

OpenPuff allows users to hide data in more than a single carrier file. It supports following carrier file format such as

- Images: BMP, JPG, PNG, TGA
- Audios: Aiff, Mp3, Wav
- Videos: 3gp, Mp4, Mpeg I, Mpeg II, Vob
- Flash-Adobe Flv, Pdf, Swf

Stegsecret

Source: http://stegsecret.sourceforge.net

Stegsecret is a steganalysis tool, which detects the hidden information in different digital media such as images, audio and video files.

PSM Encryptor

Source: http://www.programsbase.com

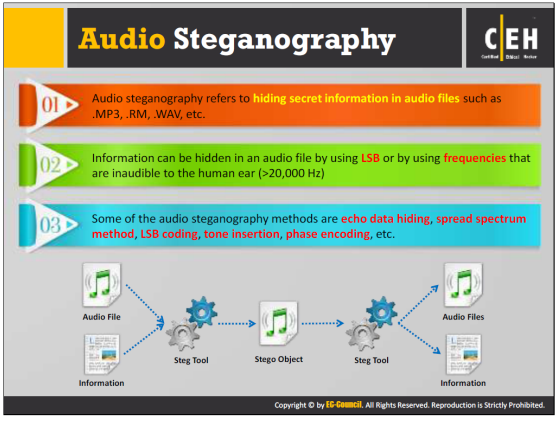
PSM Encryptor is a cryptography and steganography tool. PSM Encryptor will encrypt any group of files (including whole directory structures), but will also disguise the resulting encrypted archive as a working sound or image file.

Hidden Data Detector

Source: http://www.digitalconfidence.com

Hidden Data Detector™ is a utility designed to find and identify hidden file data and metadata. It can analyze Microsoft Office® documents (Word, Excel®, PowerPoint®), OpenOffice.org / StarOffice™ documents, JPEG, JPEG 2000, PNG, and SVG image files, AVI and MP4 video files, and WAV/MP3 audio files.

With Hidden Data Detector™, you can assess the risk of sharing files that contain potentially confidential and private hidden data, and evaluate your need for a comprehensive hidden data removal solution.



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 slight change in the audio file that go unnoticed upon listening. You can hide information in an audio file by replacing LSB or by using frequencies that are not audible to the human ear (>20,000 Hz).

Audio Steganography Methods

There are certain methods available to conceal your secret messages in audio files. Some methods implement the algorithm that relays 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 spread 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, 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.

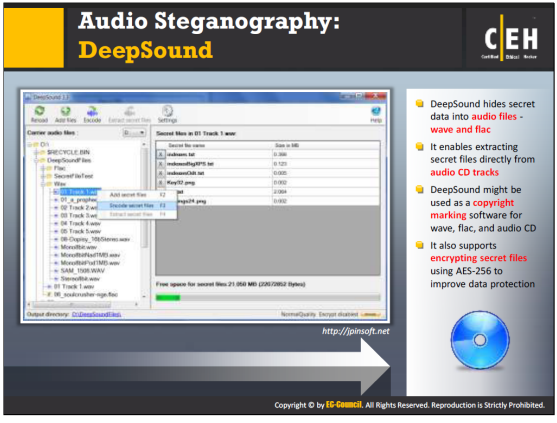
- **Tone Insertion**

  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 the 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.



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).

Source: http://jpinsoft.net

Besides DeepSound, 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:

Mp3stegz

Source: *http://mp3stegz.sourceforge.net*

mp3stegz is an application that applies steganography algorithm in mp3 files. mp3stegz will maintain original mp3 file's size and sound quality. The hidden message is compressed (zlib) and encrypted using Rijndael algorithm.

MAXA Security Tools

Source: *http://www.maxa-tools.com*

MAXA Security Tools is a package containing multiple effective tools for computer security in Windows. Steganography is one of the modules of the MAXA security tools that hide files into JPEG images and WAVE audio files. These container files appear inocuous and are thus far less likely to arous suspicion.

BitCrypt

Source: *http://bitcrypt.moshe-szweizer.com*

BitCrypt is an encryption utility that allows for storage and transmission of information in an undetectable manner. The software helps in storing plain text and hiding it from any third party, or sending information through the means provided by the Internet. The software

processes the user-supplied text: firstly encrypting it with the ciphers, and subsequently storing it in a user selected bitmap image.

MP3Stego

Source: http://www.petitcolas.net

MP3Stego hides information in MP3 files during the compression process. The data is first compressed, encrypted, and then hidden in the MP3 bit stream.

Hide4PGP

Source: http://www.heinz-repp.onlinehome.de

Hide4PGP is a software program used to hide any data in a way that the viewer or listener does not recognize any difference. Hide4PGP supports file formats such as BMP, WAV, and VOC to hide secret information.

CHAOS Universal

Source: http://safechaos.com

CHAOS Universal hides secret information in sound, image, and text files (BMP, WAV, TXT, HTML). It can also encrypt the sensitive data before transmission.

SilentEye

Source: http://www.silenteye.org

SilentEye hides messages into pictures or sounds. It also encrypts information using AES128 and AES256 algorithms. It provides interface and integration of new steganography algorithm and cryptography process by using a plug-in system.

QuickCrypto

Source: http://www.quickcrypto.com

QuickCrypto conceals sensitive data (text and files of any type) into innocent "carrier" files: JPEG, GIF, BMP, MP3 and WAV. It also encrypts every kind of file format, whether it is text, video, picture, document or audio - any type of file, on USB, floppy, thumb/flash or hard drives.

CryptArkan

Source: http://www.kuskov.com

CryptArkan encrypts and hides data files and directories inside one or more container files, such as sound/music and images. The tool can read hidden data directly from an audio CD.

StegoStick

Source: http://stegostick.sourceforge.net

The StegoStick allows users to hide any file into any file. It is based on image, audio, video steganography that hides any file or message into an image (BMP, JPG, GIF), audio/ video (MPG, WAV, etc.) or any other file format (PDF, EXE, CHM etc.)

Invisible Secrets 4

Source: http://www.invisiblesecrets.com

Invisible Secrets 4 not only encrypts your data and files for safe keeping or for secure transfer across the net; it also hides them in places that on the surface appear totally innocent, such as picture or sound files, or web pages. Even an attacker could not locate sensitive information. This software allows you to encrypt and hide documents directly from Windows Explorer, and then automatically transfer them by email or via the Internet.

Features:

- It offers file and folder encryption using 8 strong encryption algorithms (AES - Rijndael, Twofish, RC 4, Cast128, GOST, Diamond 2, Sapphire II, Blowfish)
- The software hides user's sensitive data into innocent carriers (JPEG, PNG, BMP, HTML and WAV) so that nobody can find them
- It is capable to create a package with encrypted content and to send it by e-mail
- With Invisible Secrets 4, you can store passwords in encrypted password lists and generate real-random passwords

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. In addition to Invisible Secrets 4, you can use the following tools as folder steganography tools to hide your secret information in folders:

Folder Lock

Source: http://www.newsoftwares.net

Folder Lock is a file-security application that lets you password-protect files, folders and drives; encrypt your important files on-the-fly; backup them in real-time; protect USB drives and portable devices; shred files; and clean history.

A+ Folder Locker

Source: http://www.giantmatrix.com

With A+ Folder Locker, you can store files, folders, drives, and even complete software programs in special data storage "lockers." These lockers not only secure the display of names of the files and folders you store, the robust level of security of the lockers makes them virtually impossible to break into.

A+ Folder Locker includes a variety of other high-level security features that you can use to protect the information on your computer. Features like Disguise & Hide, allow you to hide files and folders inside photos and other images on your computer.

Toolwiz BSafe

Source: http://www.toolwiz.com

ToolWiz Bsafe is encryption system, which uses AES 256 encryption to provide protection. It provides A safe is a virtual encrypted disk within a file and you can mount it as a real disk. With ToolWiz BSafe, you can create as many virtual safes as you want in the system. Once created, you can automatically mount your new safe as a drive.

Hide Folders 2012

Source: http://fspro.net

Hide Folders enables you to password protect all the private information on your hard drive. You can make your files and folders inaccessible, invisible or protect them from modification or removal. The protected folders or files are not accessible by users—no matter how they are trying to get in—locally or from the net.

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; hide 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 password.

Universal Shield

Source: http://www.everstrike.com

Universal Shield hides files, folders, and drives, and set access rules using flexible security combinations for your most precious data. You can password-protect your data, program start-up, or program uninstallation. It also contains a wizard, which includes an option of restricting personal folders and settings, as well as files/folders/drives protection, a hiding expert, and a data encryption master.

WinMend Folder Hidden

Source: http://www.winmend.com

WinMend Folder Hidden is a file/folder hiding tool. It can quickly hide files and folders on local partitions and/or on removable devices. The hidden files/folders are not visible even if users access it in another operating system on the same computer. You can view the hidden data only with a valid password. The data is invisible to other programs or on other operating systems.

Encrypted Magic Folders

Source: http://www.pc-magic.com

Encrypted Magic Folders (EMF) makes selected folders and files invisible to others, but decrypts and encrypts the files automatically and transparently as you use them.

EMF allows you to enter the password once and all your invisible folders become instantly visible and accessible.

QuickCrypto

Source: http://www.quickcrypto.com

QuickCrypto file encryption prevents anyone using a file, seeing what it contains or even understanding what type of file it is. It uses the algorithms and techniques to ensure the safety of your email communication, passwords, all confidential files and information. It hides text messages or files within a picture image or sound file. Only other QuickCrypto users can access the information.

Max Folder Secure

Source: http://www.maxfoldersecure.com

Max Folder Secure allows you lock/hide your files, folders with your personal password. Max Folder Secure is a program for password-protecting files and folders. It prevents unauthorized access to users' important information and programs. The software makes the protected folders completely invisible, inaccessible or accessible in the read-only mode.

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 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.

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 image which contains hidden message to another person through email or just save it to the photo library

- Reveal the hidden message from the image

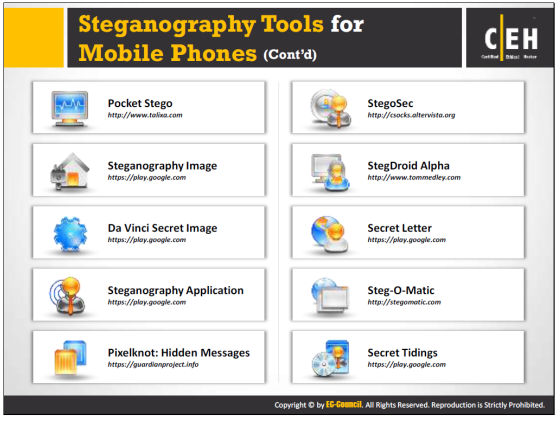
SPY PIX

Source: http://www.juicybitssoftware.com

Spy Pix helps in hiding and sending secret messages in plain view, and hiding one image inside of another decoy image.

Features:

- Ability to select hidden and decoy images from your photo album
- Support for the built-in camera
- Simple slider control to easily blend the hidden and decoy images



Below is the list of steganography tools for mobile phones:

Pocket Stego

Source: http://www.talixa.com

Pocket Stego is an Android steganography tool. You can use it to add messages to images, or to extract messages from images. It uses 7-bit ASCII or 8-bit ASCII and options to invert or reverse bits to obscure your communication.

Steganography Image

Source: https://play.google.com

Steganography Image is an image steganography tool for mobile phones that allows you to hide any text in an image, using the PVD (Pixel Value Differencing) algorithm.

Da Vinci Secret Image

Source: https://play.google.com

Da Vinci Secret Image mobile app hides your secret message inside an image and sends it to a target mobile user. Everybody will see a cool picture without being aware of messages hidden inside it and only the recipient is able to read the hidden message by using the same application. You can also specify a password to increase security.

Steganography Application

Source: https://play.google.com

Steganography Application app embeds secret messages in images. It embeds images in images and videos. It also retrieves the embedded message from image and the embedded images from images and videos.

Pixelknot: Hidden Messages

Source: https://guardianproject.info

Pixelknot is an Android application that allows users to hide short text-based messages in photographs and share them across trusted channels.

StegoSec

Source: http://csocks.altervista.org

Stegosec is a secure personal data and information transfer security software. Stegosec can hide a text into an image acquired from the internal camera or also from your image library. It is impossible to retrieve the text message from the resulting image and both the images are visibly identical.

StegDroid Alpha

Source: http://www.tommedley.com

StegDroid Alpha records audio, and embeds a secret text message into the audio file. You can then share the recording with others, who can extract the secret message with the same app. The tool encrypts the messages with a password for extra security.

Secret Letter

Source: https://play.google.com

Secret Letter is an android application that provides a new method for applying the art of steganography: it hides your message into the images or photos taken by the phone's camera.

Steg-O-Matic

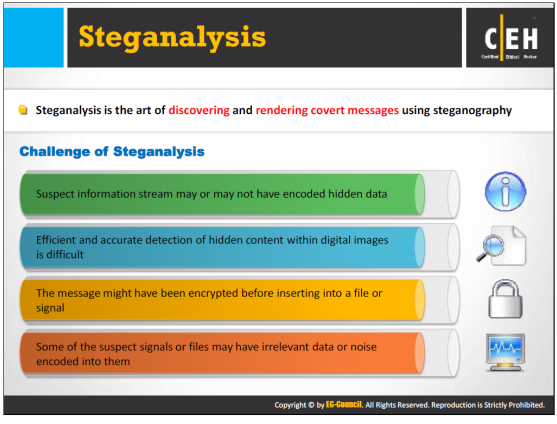
Source: http://stegomatic.com

With the Steg-O-Matic app, you can send a secret message or secret photo by hiding it inside of a "decoy" image. You can then send this cover image via email, social media, or post it on your public blog—no one will know that it contains a covert message or image.

Secret Tidings

Source: https://play.google.com

Secret Tidings mobile application hides messages in plain images. No one but the receiver will be able to read the message. Secret Tidings allows you to compose messages with text and attachments and hides those messages in images. The tools the hidden messages with a password.



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 steganalyst tries to detect the hidden messages embedded in images, text, audio and video carrier mediums using steganography. It 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.

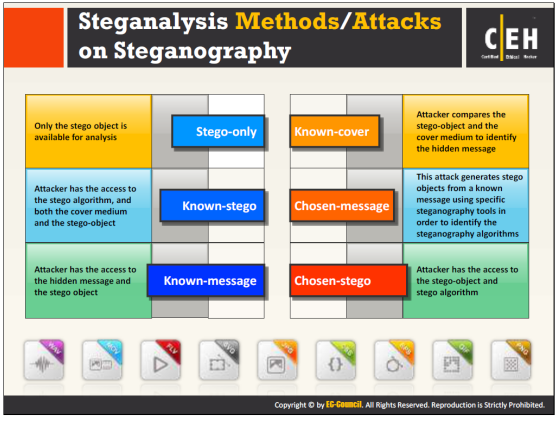
Steganalysis contains two aspects: the ***detection*** and ***distortion*** of messages. In the detection phase, the analyst observes the relationships between the steganography tools, stego-media, cover and message. In the distortion phase, the analyst manipulates the stego-media to extracts the embedded message is whether useless or remove it 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 cover image and 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.



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 attack: 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 algorithms and related attacks to recover the 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**

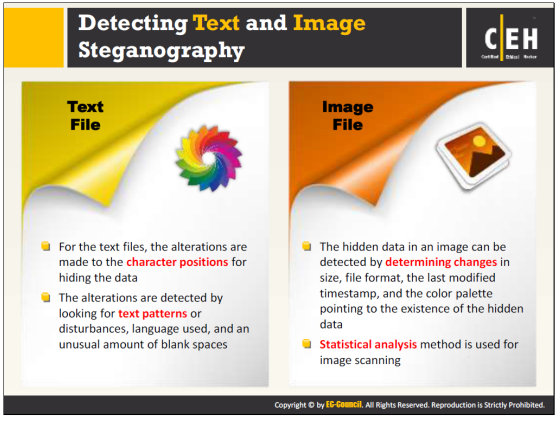
  Attackers use the known-cover attack when they have knowledge of both the stego-object and the original cover-medium. This will enable a comparison between both the mediums in order to detect the changes in the format of the medium and find the hidden message.

- **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.



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 text files, alter the character position 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 sometime as it displays the spaces, tabs, and other characters that distort the text's presentation during text steganography.

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

  - Unusual patterns used in stego object
  - Appended extra spaces
  - Invisible characters

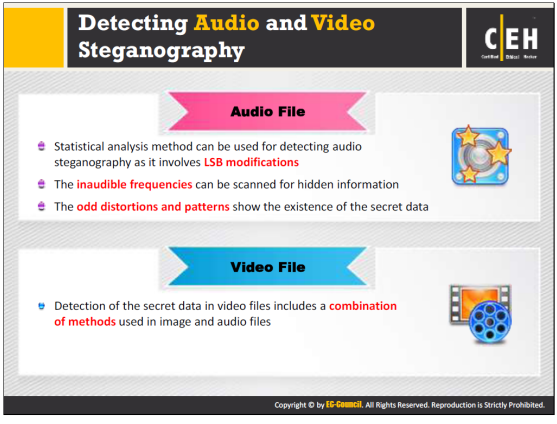
Image Files

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.



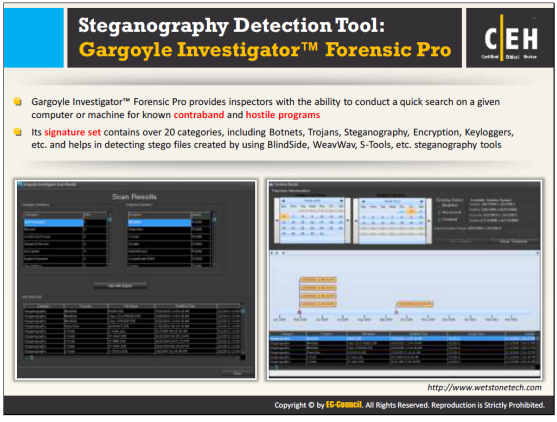
Both audio and video steganography is quite difficult to detect, as compared to other types such as image, and document. Moreover, it is very hard to detect good steganography of any type. However, careful analysis of audio and video signal for hidden information may create chances of detecting it correctly.

- **Audio File**

  Audio steganography is a process of embedding confidential information such as private documents and files in digital sound.

- **Video File**

  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.

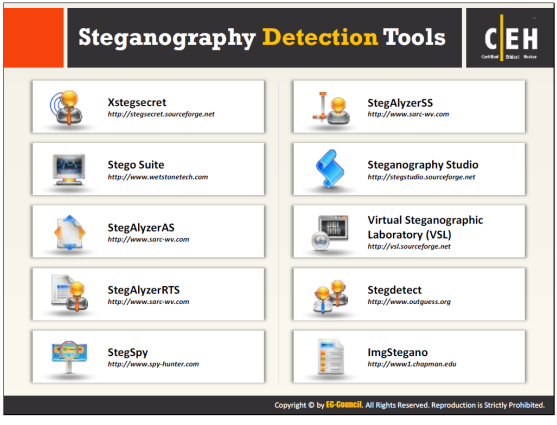


Gargoyle Investigator™ Forensic Pro is a tool that conducts quick searches on a given computer or machines for known contraband and malicious programs. The tool can find remnants in a removed program as it conducts the search for the individual files associated with a particular program. Its signature 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 cable to scan on a stand-alone system or network resource for known contraband and hostile programs
- It consists of 20 datasets containing over 20,000 types of malicious software
- 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 customizable

Source: http://www.wetstonetech.com



Steganography detection tools allow you to detect and recover hidden information in any digital media such as images, audio, and video. The following is a list of some steganography detection tools that may help you in detecting steganography in target cover medium:

Xstegsecret

Source: http://stegsecret.sourceforge.net

Xstegsecret allows the detection of hidden information by using the most known steganography methods. With the help of this tool, it is possible the detection of hidden information in different digital media such as images, audio and video. It detects EOF, LSB, DCTs and other techniques.

Stego Suite

Source: http://www.wetstonetech.com

Stego Suite™ includes various sets of tools that can help you to detect hidden information from steganography. It includes tools such as Stego Hunter, Stego Watch, Stego Analyst, and Stego Break.

StegAlyzerAS

Source: http://www.sarc-wv.com

StegAlyzerAS is a steganalysis tool designed to extend the scope of traditional computer forensic examinations by allowing the examiner to scan suspect media or forensic images of suspect media for known artifacts of over 1,225 steganography applications.

StegAlyzerRTS

Source: http://www.sarc-wv.com

StegAlyzerRTS is the network security appliance capable of detecting digital steganography applications and the use of those applications in real-time. It detects insiders downloading steganography applications by comparing the file fingerprints, or hash values, to a database of known file, or artifact, hash values associated with over 1,225 steganography applications.

StegSpy

Source: http://www.spy-hunter.com

StegSpy is a program that allows identification of a "steganized" file. StegSpy will detect steganography and the program used to hide the message. It also identifies the location of the hidden content and identifies specific versions of the steganography programs used.

StegAlyzerSS

Source: http://www.sarc-wv.com

StegAlyzerSS is a steganalysis tool designed to extend the scope of traditional computer forensic examinations by allowing the examiner to scan suspect media or forensic images of suspect media for over 55 uniquely identifiable byte patterns, or known signatures, left inside files when particular steganography applications are used to embed hidden information within them.

Steganography Studio

Source: http://stegstudio.sourceforge.net

Steganography Studio software is a tool to learn, use and analyze key steganography algorithms. It implements several algorithms highly configurable with a variety of filters. It also implements the best image analysis algorithms for the detection of hidden information.

Virtual Steganographic Laboratory (VSL)

Source: http://vsl.sourceforge.net

The VSL application helps in hiding data in digital images, detect its presence and test its robustness using any number of different adjustable techniques. VSL provides a framework to use multiple methods at the same time. It can perform complex processing in both batch and parallel form.

Stegdetect

Source: http://www.outguess.org

Stegdetect is an automated tool for detecting steganographic content in images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images. Given a set of normal images and a set of images that contain hidden content by a new steganographic application, Stegdetect can automatically determine a linear detection function that is applicable to yet unclassified images.

ImgStegano

Source: http://www1.chapman.edu

ImgStegano helps you in detecting steganography on bmp or png image. It uses an Enhanced LSB technique to detect image steganography.

In the previous section, we have seen how an attacker hides malicious files on a target computer using various steganographis techniques, rootkits, 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 trace back. This starts with erasing the contaminated logs and possible error messages generated in 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 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. There are also such tools for the NT operating system. 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 attacker perform toward removing his/her traces on the computer are:

- **Disable auditing:** Attacker disables auditing features of the target system
- **Clearing logs:** Attacker clear/delete the system log entires corresponding to his/her activities
- **Manipulating logs**: 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.

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 as category and sub-category level. 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
```

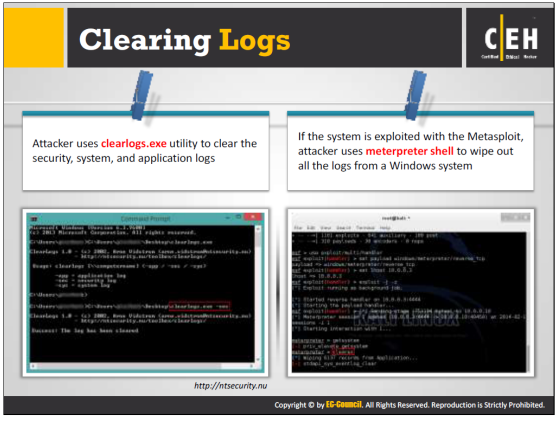
This will make changes in the various logs that might register the attacker's actions. He/she can choose to hide the registry keys changed later on.

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:*
```

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



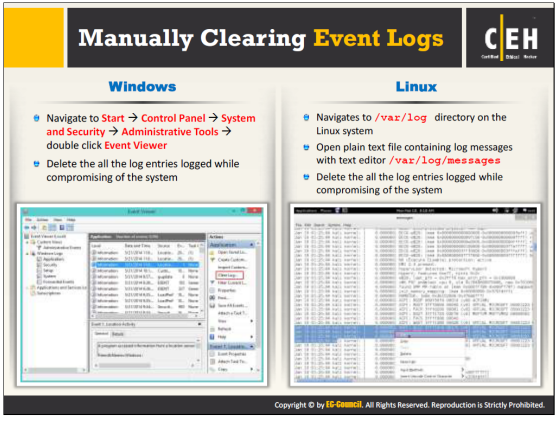
The clearlogs.exe is a utility that can be used to wipe out the logs of the target system. This utility need to run through command prompt to delete security, system, and application logs on the target system. Attackers might use this utility, wiping out the logs as one method of covering their tracks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

Steps to clear logs using clearlogs.exe utility:

1. Download the **clearlogs.exe** is utiliy from the 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

When malicious activities are performed on the system with Metasploit Framework, the Logs of the target system can wipe out as follows:

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



Once attackers gain administrative access to a target system, they can then manually wipe out the log entries corresponding to their activities on both Windows and Linux computer. Refer to the slide on how to clear event logs on Windows and Linux operating systems, respectively.

Attacker clears 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. Refer to the slide on how to clear online tracks from the Privacy Settings or from the Windows registry (Windows 8.1).

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. It 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
- **Registry Cleaner:** Advanced features to remove unused and old registry entries

Source: http://www.piriform.com

MRU-Blaster is a program used to detect and clean MRU (most recently used) lists on computers. It cleans up tens of thousands of "**usage tracks**" and other remnants that most programs leave behind. MRU list provides you with the complete information about the names, locations of the last files you have accessed, opened, saved, and looked at. It ensures your Internet privacy. It allows you to clean out your temporary Internet files and cookies.

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

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. Other than those discussed in the previous page, there are some more Track covering tools discussed here that could help to delete the traces of attacker.

Wipe

Source: http://privacyroot.com

Wipe is a program that can remove many gigabytes of garbage on the computer. It removes records about personal activity on the PC. It allows you to delete browser history and cache, index.dat files, registry, Internet cookie files, autocomplete-history, temporary Internet files, and so on.

Tracks Eraser Pro

Source: http://www.acesoft.net

Tracks Eraser Pro removes traces of your activity left on the Internet and your computer after you have been using it. It runs through all the major areas on your computer where evidence of your activity might be left, identifying it and erasing it securely.

BleachBit

Source: http://bleachbit.sourceforge.net

BleachBit frees cache, delete cookies, clear Internet history, shred temporary files, delete logs, and discard junk. It wipes clean a thousand applications including Firefox, Internet Explorer, Adobe Flash, Google Chrome, Opera, Safari, and more. It wipes free disk space to hide traces of files deleted by other applications.

AbsoluteShield Internet Eraser Pro

Source: http://www.internet-track-eraser.com

AbsoluteShield Internet Eraser cleans up all the tracks of your Internet and computer activities. It can erase the browser cache, history, cookies, typed URLs, autocomplete list. With the plugin support, it erases the tracks left by any applications.

Clear My History

Source: http://www.hide-my-ip.com

Clear My History tool cleans all history of your web browsing and computer usage. It wipes activity history of dozens of programs such as Firefox, Internet Explorer, Windows Media Player, Yahoo, MSN, and Google.

ClearProg

Source: http://www.clearprog.de

ClearProg allows you to erase the cache, cookies, history, typed URLs, autocomplete memory, index.dat from your browsers, and Window's temp folder, run history, search history, recycle bin, and recent documents. It can delete your Internet usage history and help you clean the tracks of popular programs.

WinTools.net Professional

Source: http://www.wintools.net

WinTools.net Professional is a suite of tools used to remove unwanted software from disk drives and dead references from the Windows registry. It puts you in control of the Windows start up process, memory monitoring and gives you the power to customize desktop and system settings to fit your needs, ensures your privacy and keep sensitive information secure.

RealTime Cookie & Cache Cleaner (RtC3)

Source: http://www.kleinsoft.co.za

This application cleans up your cookies and caches in real time while you surf the Web. It displays the number of cookies on your computer, and effectively removes them. The program lists the names and filenames of the cookies and cache files it deletes, and you can selectively save cookies in the Cookie Jar.

Privacy Eraser

Source: http://www.cybertronsoft.com

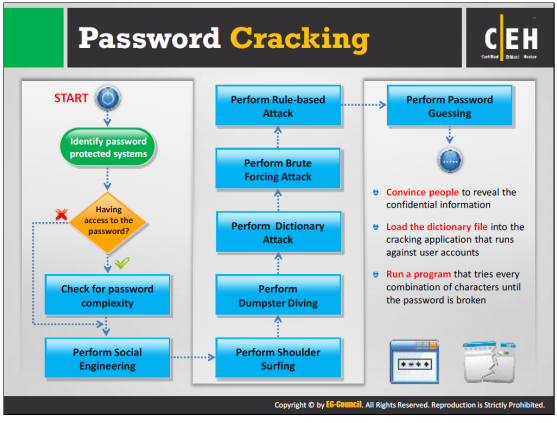
Privacy Eraser cleans up all your Internet history tracks and past computer activities. It can quickly erase the Internet cache, cookies, browsing history, address bar history, typed URLs, autocomplete form history, saved password and index.dat files of your browser, and Windows run history, search history, open/save history, recent documents, temporary files, recycle bin, clipboard, taskbar jump lists, DNS cache, log files, memory dumps, error reporting, and much more.

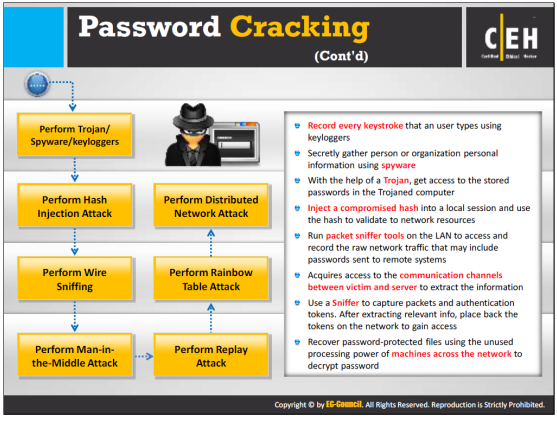
Free Internet Window Washer

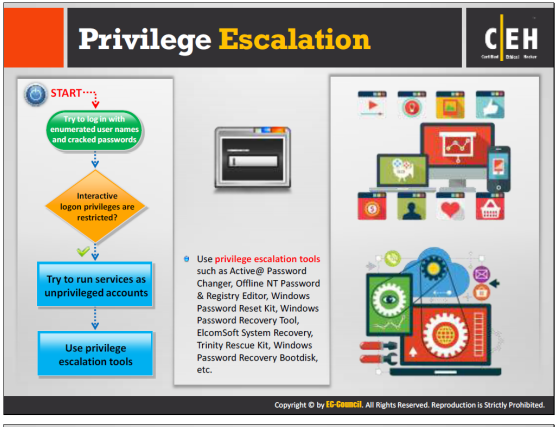
Source: http://www.eusing.com

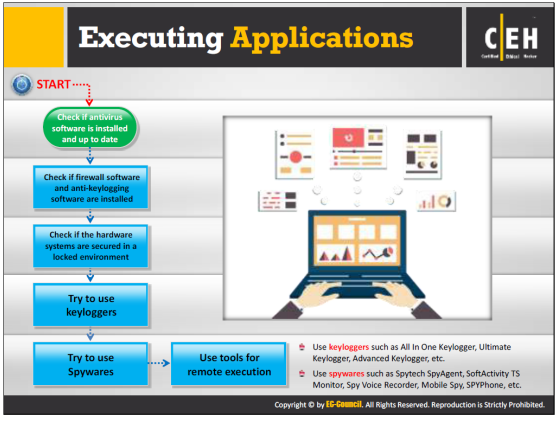
Free Internet Window Washer is an Internet tracks eraser and privacy cleaner software. It can erase your Internet tracks, computer activities and programs history information stored in many hidden files on your computer. It also provides you option to clean the data from your PC more securely and permanently, and erases Windows temp folders, run history, search history, open/save history, recent documents, your browser's cache, cookies, history, visited URLs, typed URLs, auto complete memory, index.dat files, and much more.

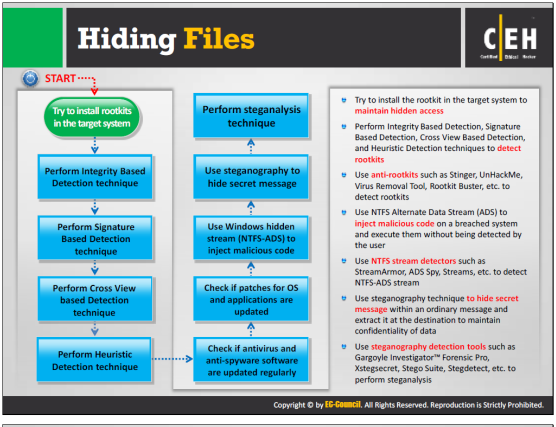
Pen testers use their system hacking knowledge to assess the security of target systems. As a pen tester, you should evaluate the security posture of your target system, by trying to break its security through simulating various attacks in the same way an outside attacker would do. There are certain 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.

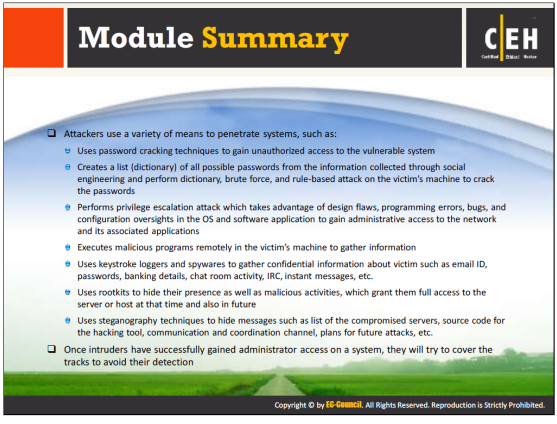












In this module, you have learned about the various tools, techniques, and methodology that hackers use to breach system security. Then we also explored the pen-testing step for assessing target system security.