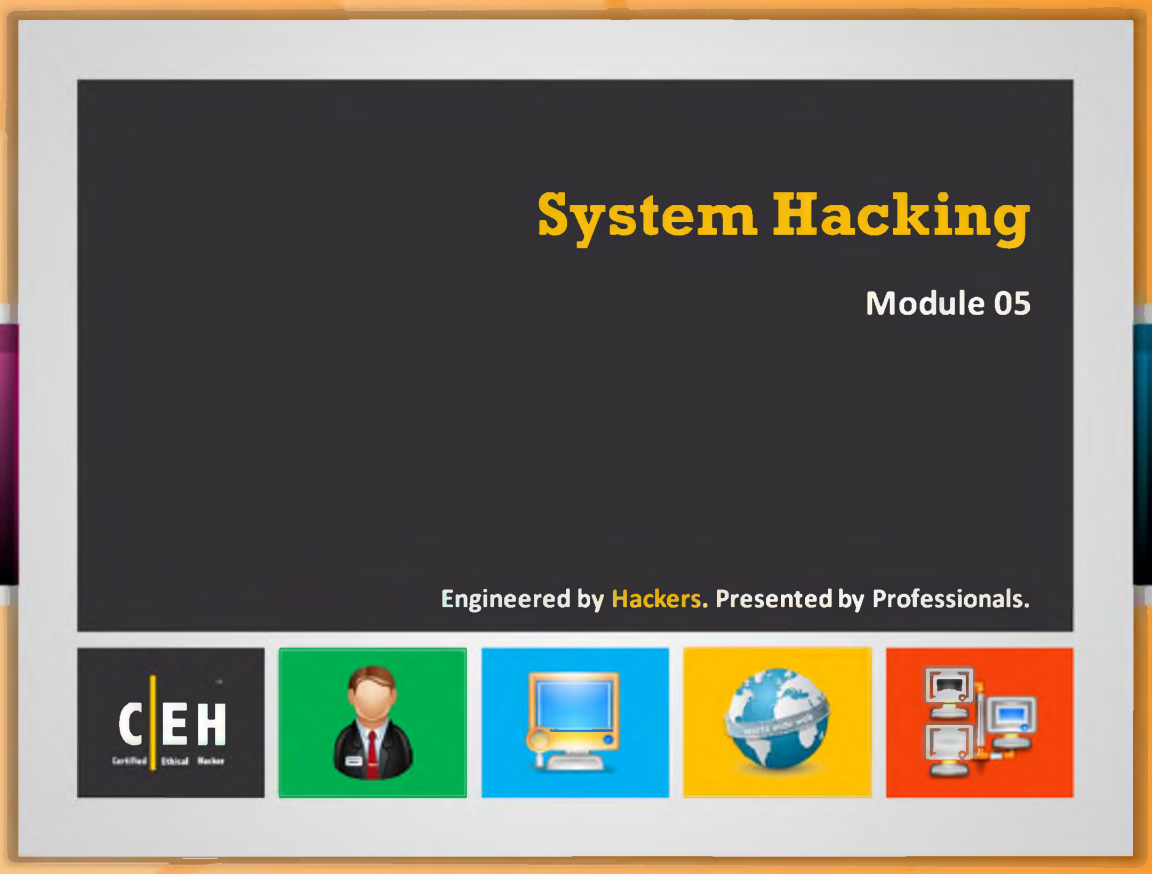
System Hacking

Module 05



Ethical Hacking and Countermeasures v8

Module: 05 System Hacking

Exam 312-50

Security News

IEEE Hack Confirmed, 100k Plain Text Passwords Vulnerable

Source: http://www.kitguru.net

After details were revealed by Radu Dragusin over at IEEElog.com recently that passwords and user details for some **100,000** members of the **Institute of Electrical** and **Electronics Engineers** had been made publicly available on the company's FTP server for at least a month, the organization confirmed this in a **communication** to members, advising them to change their details immediately.

The IEEE is an organization that is designed to advance technology and has over 400,000 members worldwide, many of those including employees at Apple, Google, IBM, Oracle, and Samsung. It is responsible for globally used standards like the **IEEE 802.3 Ethernet standard** and the IEEE 802.11 Wireless Networking standard. At an organization like this, you'd expect security to be high.

Still, this hack was no hoax. The official announcement of it reads: "IEEE has become aware of an incident regarding **inadvertent** access to **unencrypted log files** containing **user IDs** and

passwords. This matter has been addressed and resolved. None of your financial information was made accessible in this situation."

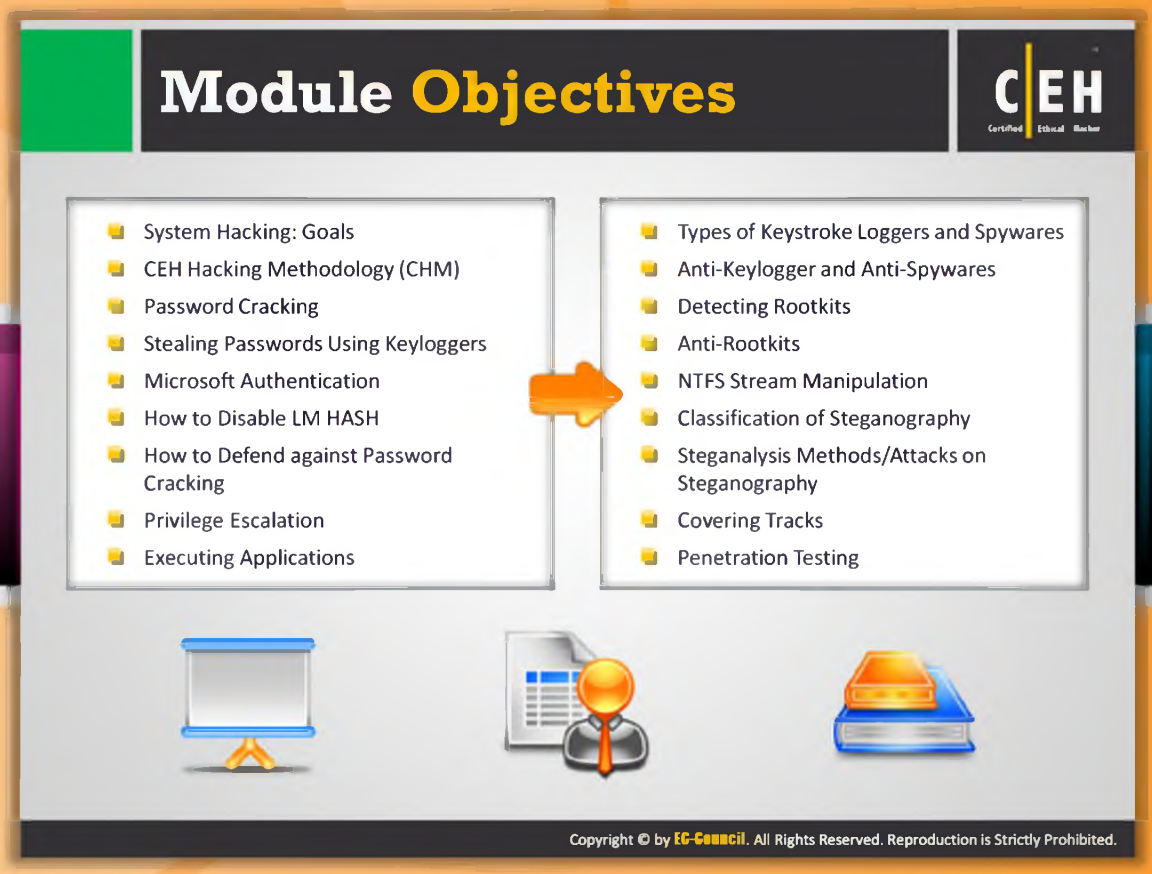
The company continued saying though, that it was technically possible that during the time this information was available, that someone could have used it to access a user's account and therefore, as a "precautionary measure," the IEEE recommended all users change their account information. Until that time, users were not be able to access their account at all.

In what seems like quite a bold move, the organization went on to explain to users that one of the best ways to protect themselves is to use a strong, unique password for their login. Considering it was an IEEE security blunder that caused the hack, advising other people on password strength seems a bit hypocritical.

That said, in Mr Dragusin's reveal of the hacked information, he produced a graph detailing some of the most commonly used passwords. Almost 300 people used "123456" and other variations of numbers in that same configuration, while hundreds of others used passwords like "admin," "student," and "ieee2012." Considering the involvement of IEEE members in pushing the boundaries of current technology, you'd assume we wouldn't need to turn to Eugene "The Plague" Belford to explain the importance of password security.

Author: Jon Martindale

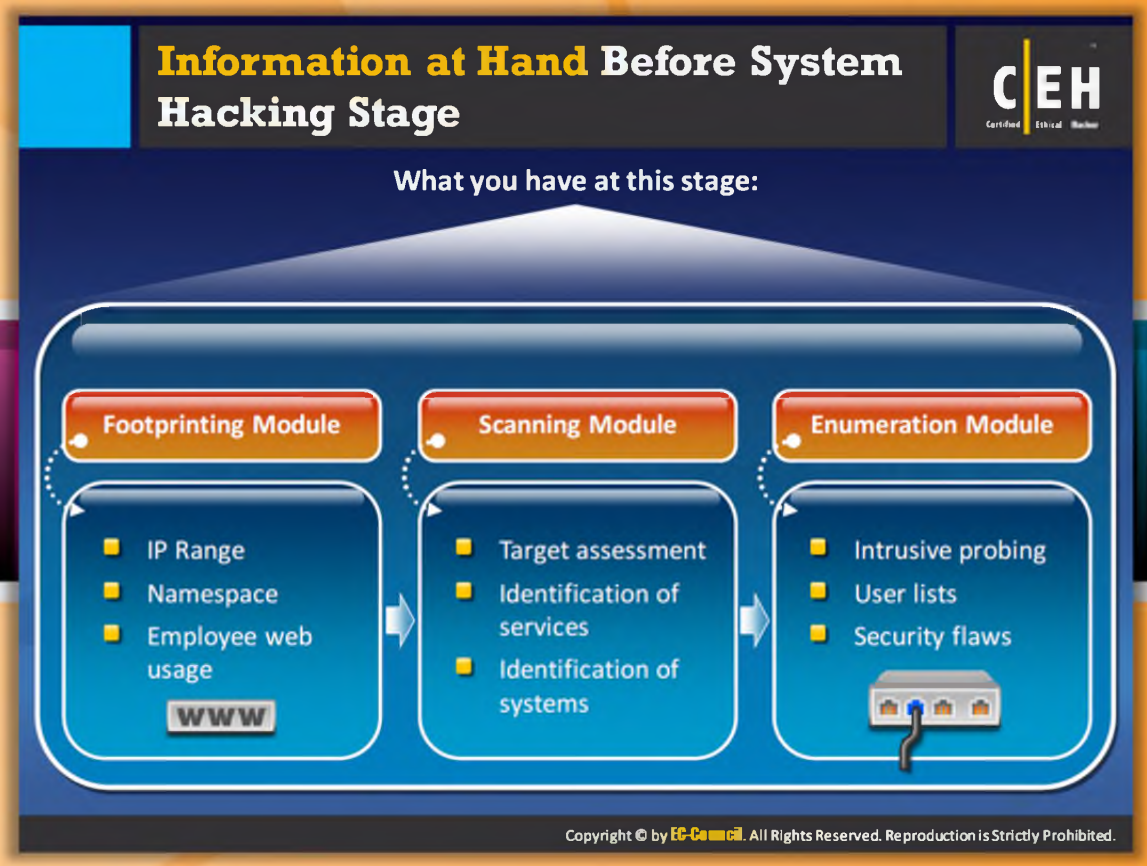
http://www.kitguru.net/channel/jon-martindale/ieee-hack-confirmed-100k-plain-text-passwords-vulnerable/



Module Objectives

The preceding modules dealt with the **progressive intrusion** that an attacker makes towards his or her target system(s). You should bear in mind that this does not indicate a **culmination** of the attack. This module familiarizes you with:

- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- Password Cracking
- Stealing Passwords Using Keyloggers
- Microsoft Authentication
- How to Disable LM HASH
- How to Defend against Password Cracking
- Privilege Escalation
- Executing Applications
- Types of Keystroke Loggers and Spywares
- Anti-Keylogger and Anti-Spywares
- Detecting Rootkits
- Anti-Rootkits
- NTFS Stream Manipulation
- Classification of Steganography
- Steganalysis Methods/Attacks on Steganography
- Covering Tracks
- Penetration Testing



Information at Hand Before System Hacking Stage

Before beginning with system hacking, let's go over the phases you went through and the information you collected so far. Prior to this module, we discussed:

Footprinting Module

Footprinting is the process of **accumulating data** regarding a specific network environment. Usually this technique is applied for the purpose of finding ways to intrude into the network environment. Since footprinting can be used to attack a system, it can also be used to protect it. In the footprinting phase, the attacker creates a profile of the target organization, with the information such as its IP address range, namespace, and **employee web usage**.

Footprinting improves the ease with which the systems can be exploited by revealing system vulnerabilities. Determining the objective and location of an intrusion is the primary step involved in **footprinting**. Once the objective and location of an intrusion is known, by using non-intrusive methods, **specific information** about the organization can be gathered.

For example, the web page of the organization itself may provide employee bios or a personnel directory, which the hacker can use it for the social engineering to reach the objective. Conducting a Whois query on the web provides the **associated networks** and **domain names** related to a specific organization.

Scanning Module

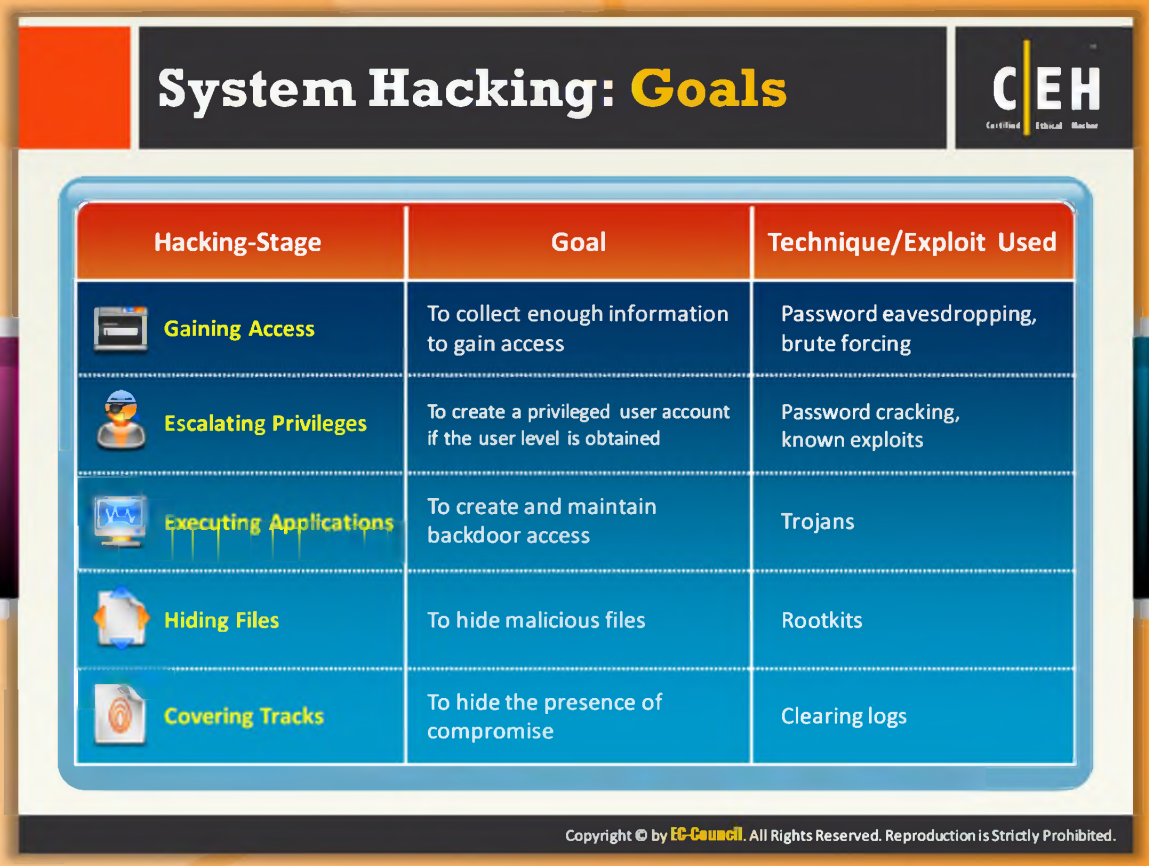
Scanning is a procedure for identifying active hosts on a network, either for the purpose of network security assessment or for attacking them. In the scanning phase, the attacker finds information about the target assessment through its IP addresses that can be accessed over the Internet. Scanning is mainly concerned with the identification of systems on a network and the identification of services running on each computer.

Some of the **scanning** procedures such as port scans and ping sweeps return information about the services offered by the live hosts that are active on the Internet and their **IP addresses**. The inverse mapping scanning procedure returns the information about the IP addresses that do not map to the live hosts; this allows an attacker to make suppositions about feasible addresses.

Enumeration Module

Enumeration is the method of intrusive probing into the target assessment 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 crosses over the target territory to unearth information about the network, and shares users, groups, applications, and banners.

The attacker's objective is to identify valid user accounts or groups where he or she can remain **inconspicuous** once the system has been compromised. **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 what the target might have made public, such as a **DNS address**; however, it is possible that the attacker stumbles upon a remote IPC share, such as **IPC$** in **Windows**, that can be probed with a null session allowing shares and accounts to be enumerated

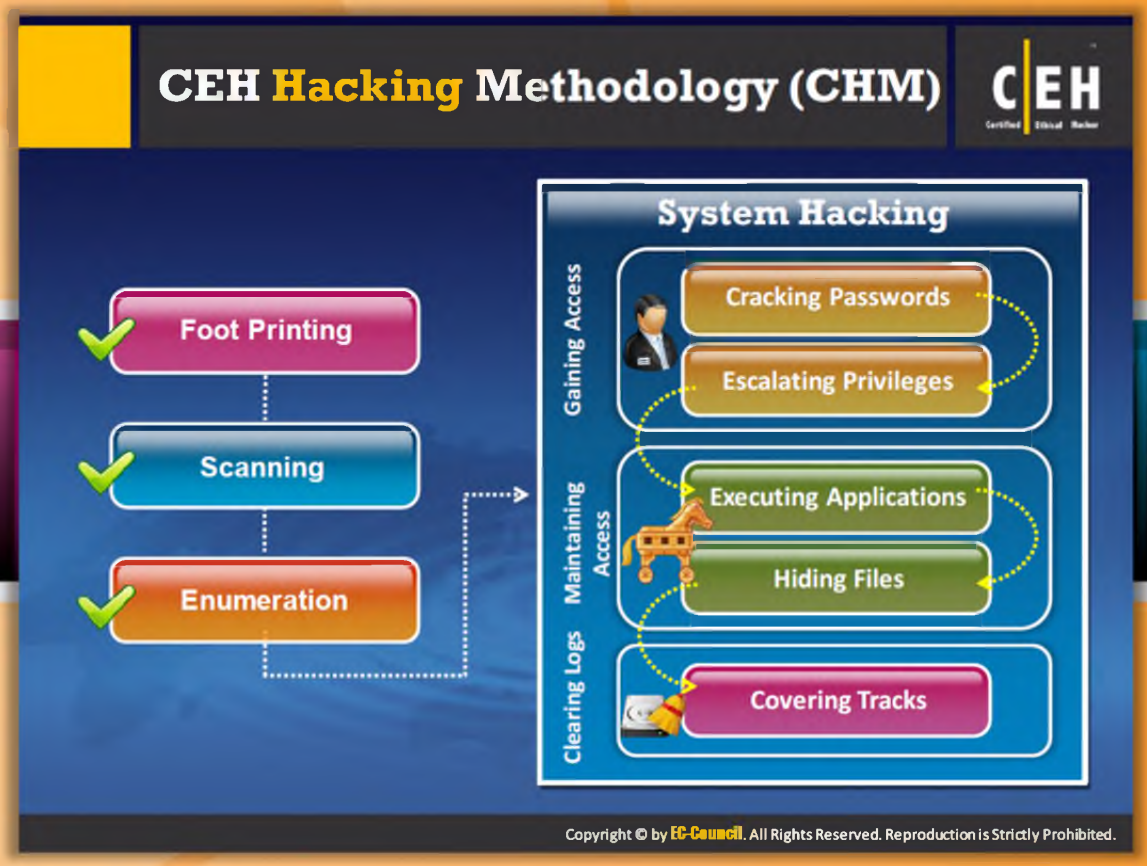


System Hacking: Goals

Every criminal commits a crime to achieve certain goal. Likewise, an **attacker** can also have certain goals behind performing attacks on a system. The following may be some of the goals of attackers in committing attacks on a system. The table shows the goal of an attacker at different **hacking stages** and the **technique** used to achieve that goal.

Hacking-Stage	Goal	Technique/Exploit Used
Gaining Access	To collect enough information to gain access	Password eavesdropping, brute forcing
Escalating Privileges	To create a privileged user account if the user level is obtained	Password cracking, known exploits
Executing Applications	To create and maintain backdoor access	Trojans
Hiding Files	To hide malicious files	Rootkits
Covering Tracks	To hide the presence of compromise	Clearing logs

FIGURE 5.1: Goals for System Hacking



CEH Hacking Methodology (CHM)

Before hacking a system, an attacker uses **footprinting**, **scanning**, and **enumeration** techniques to detect the target area of the attack and the **vulnerabilities** that prove to be **doorways** for the attacker. Once the attacker gains all the necessary information, he or she starts hacking. Similar to the attacker, an **ethical hacker** also follows the same steps to test a system or network. In order to ensure the **effectiveness** of the test, the ethical hacker follows the hacking methodology. The following diagram depicts the **hacking methodology** followed by ethical hackers:

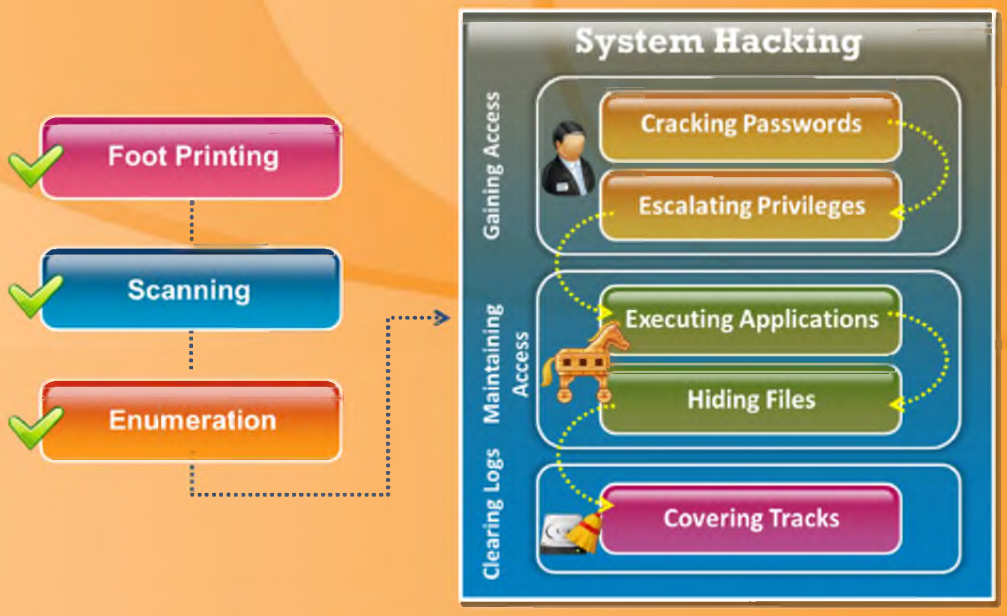
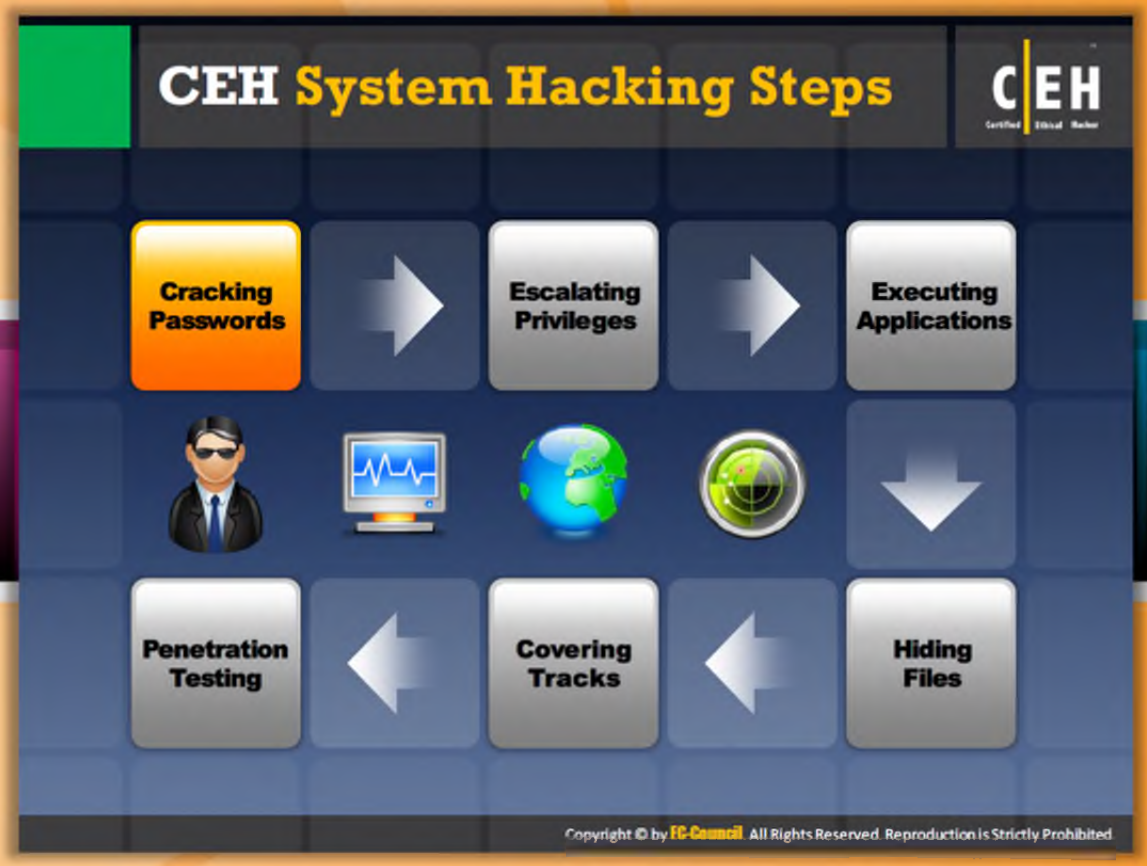


FIGURE 5.2: CEH Hacking Methodology (CHM)

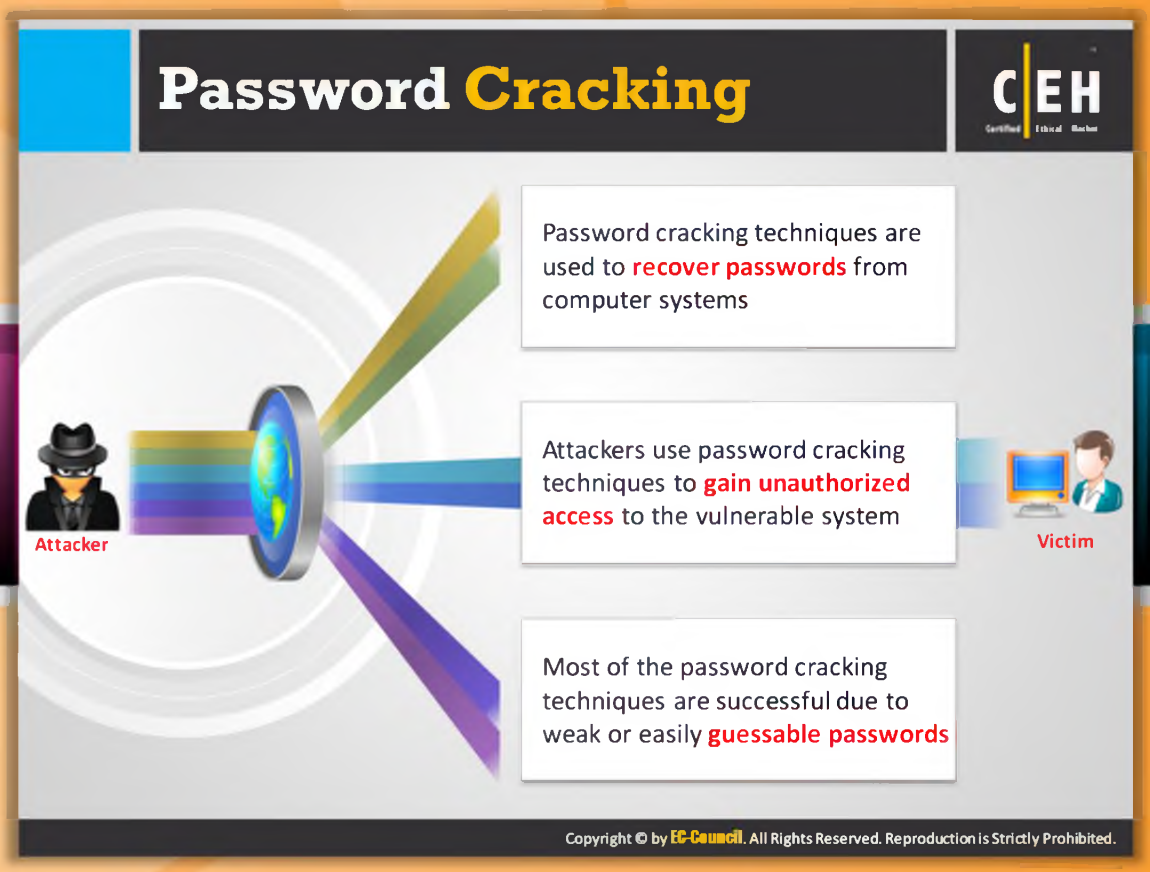


CEH System Hacking Steps

System hacking cannot be accomplished at a single go. It is accomplished through various steps that include cracking passwords, escalating privileges, executing applications, hiding files, covering tracks, and finally penetration testing. Now it's time to discuss these steps one by one thoroughly, to determine how the attacker hacks the system. In an attempt to hack a system, the attacker first tries to crack passwords.

This section describes the first step, i.e., password cracking, that will tell you how and what types of different tools and techniques an attacker uses to crack the password of the target system.

Cracking Passwords	Hiding Files
Escalating Privileges	Covering Tracks
Executing Applications	Penetration Testing

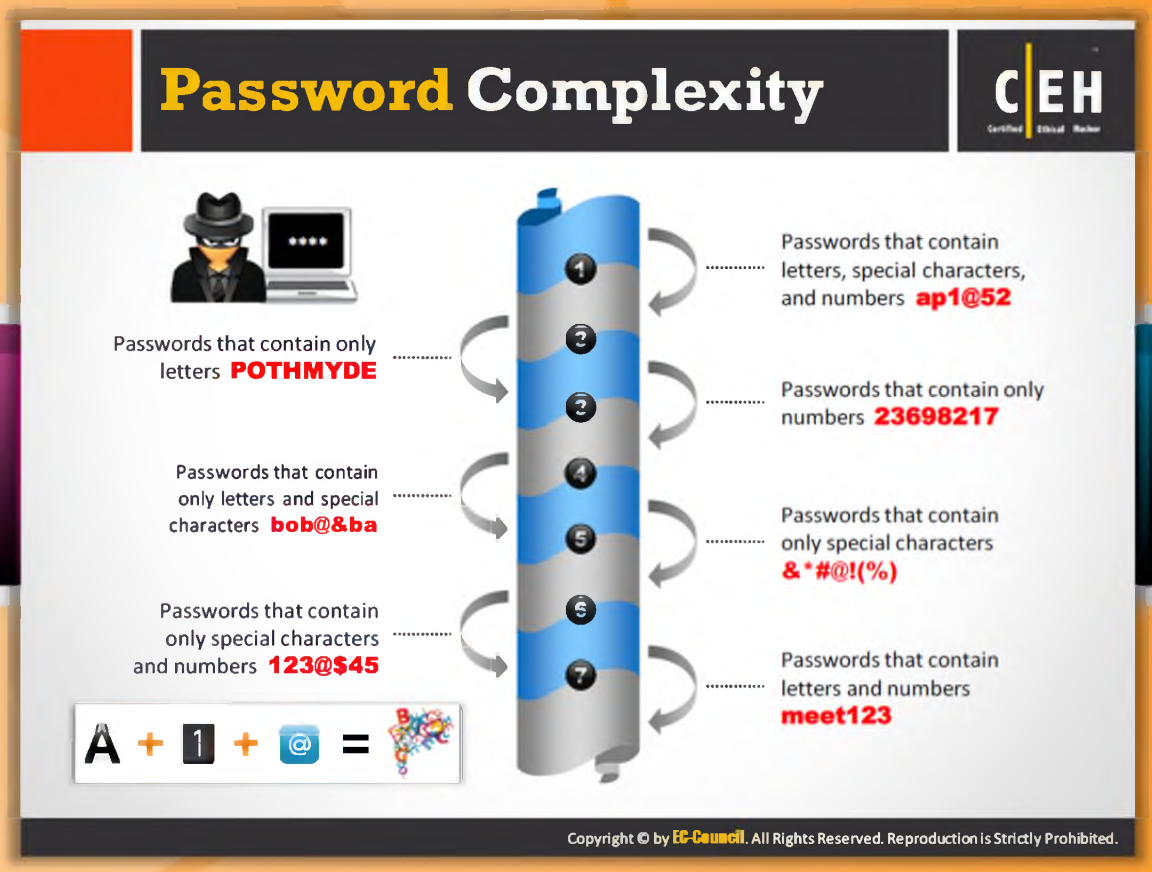


Password Cracking

Password cracking is the process of recovering passwords from the data that has been 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 the system administrators to check for easily **crackable passwords** or it can also be used to gain unauthorized access to a system.

Many hacking attempts start with password cracking attempts. Passwords are the key piece of information necessary to access a system. Consequently, most attackers use password cracking techniques to gain **unauthorized** access to the **vulnerable** system. Passwords may be cracked manually or with automated tools such as a dictionary or brute-force method.

The computer programs that are designed for cracking passwords are the functions of the number of possible passwords per second that can be checked. Often users, while creating passwords, select passwords that are **predisposed** to being cracked such as using a pet's name or choosing one that's simple so they can remember it. Most of the passwords **cracking techniques** are successful due to weak or **easily guessable passwords**.

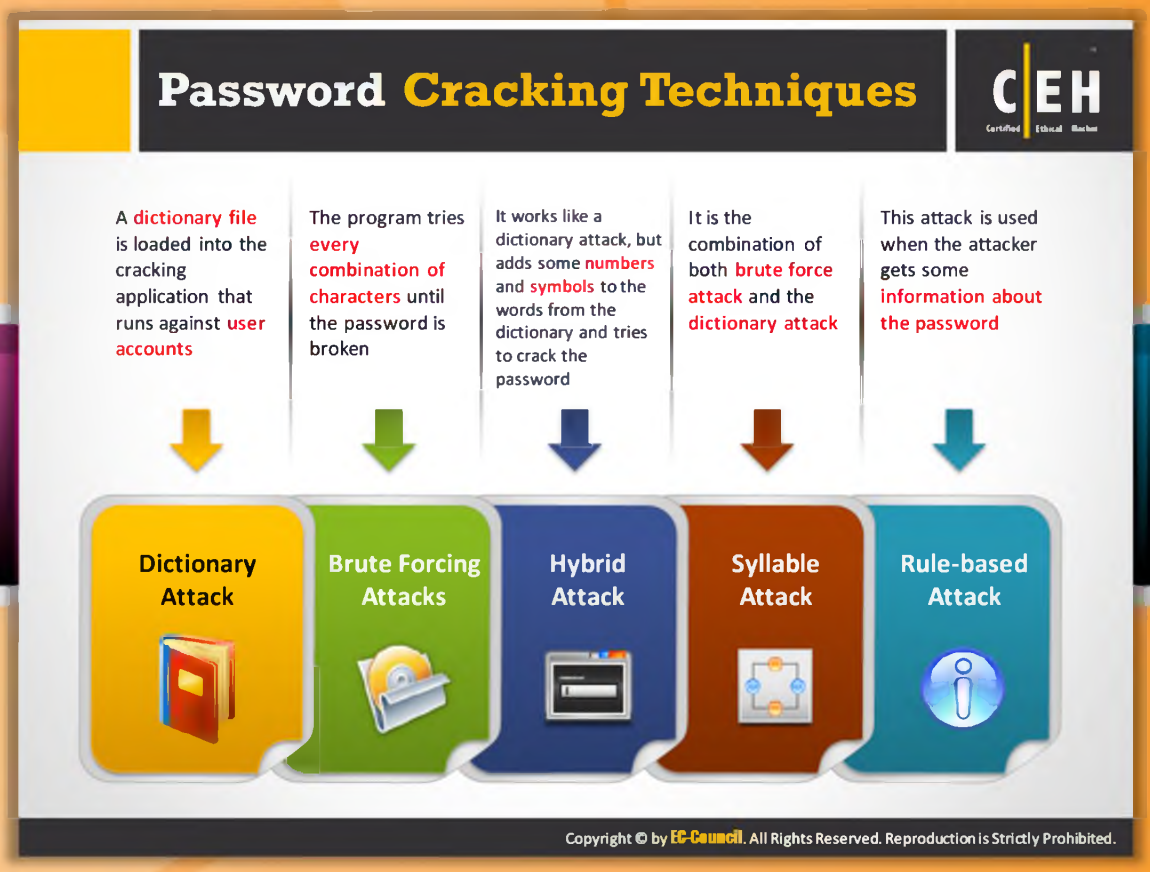


Password Complexity

Password complexity plays a key role in **improving security against attacks**. It is the important element that users should ensure while creating a password. The password should not be simple since simple passwords are **prone** to **attacks**. The passwords that you choose should always be complex, long, and difficult to remember. The password that you are setting for your account must meet the **complexity requirements policy** setting.

Password characters should be a combination **of alphanumeric characters**. Alphanumeric characters consist of letters, numbers, punctuation marks, and mathematical and other conventional symbols. See the implementation that follows for the **exact characters** referred to:

- Passwords that contain letters, special characters, and numbers: ap1@52
- Passwords that contain only numbers: 23698217
- Passwords that contain only **special characters**: &*#@!(%)
- Passwords that contain letters and numbers: meet123
- Passwords that contain only letters: POTHMYDE
- Passwords that contain only letters and special characters: bob@&ba
- Passwords that contain only special characters and numbers: 123@$4



Password Cracking Techniques

Password cracking is the technique used for **discovering passwords**. It is the classic way to **gain privileges** to a computer system or network. The common approach for cracking a password is to continually try guesses for the password with various combinations until you get the correct one. There are **five techniques** for password cracking, as follows.

Dictionary Attacks

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. The program uses every word present in the dictionary to find the password. **Dictionary attacks** are more useful than brute force attacks. But this attack does not work with a system that uses **passphrases**.

This attack can be applied under two situations:

- In cryptanalysis, it is used to find out the decryption key for **obtaining plaintext** from ciphertext.
- In computer security, to avoid **authentication** and access the computer by **guessing passwords**.

Methods to improve the success of a dictionary attack:

- Use the number of dictionaries such as **Technical dictionaries** and foreign dictionaries which helps to retrieve the correct password
- Use the string manipulation on the dictionary, means if dictionary contain the word "system" then try string manipulation and use "**metsys**" and others

Brute Forcing Attacks

The **cryptographic algorithms** must be sufficiently hardened in order to prevent a brute-force attack. The definition as stated by 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."

When someone tries to produce each and every single encryption key for data until the needed information is detected, this is termed a brute force attack. Until this date, this type of attack was performed by those who had sufficient **processing power**.

The United States government once believed (in 1977) that a 56-bit **Data Encryption Standard** (DES) was sufficient to deter all brute-force attacks, a claim that several groups across the world had tested.

Cryptanalysis is a brute force attack on an encryption of a brute force search of the **keyspace**. In other words, testing all possible keys is done in an attempt to recover the plaintext used to produce a particular **ciphertext**. The detection of key or plaintext with a faster pace as compared to the brute force attack can be considered a way of breaking the cipher. A cipher is secure if no method exists to break that cipher other than the brute force attack. Mostly, all **ciphers** are deficient of **mathematical proof** of security.

If the keys are originally chosen randomly or searched randomly, the plaintext will, on average, become available after half of all the possible keys are tried.

Some of the considerations for brute-force attacks are as follows:

- It is a time-consuming process
- All passwords will eventually be found
- Attacks against NT hashes are much more difficult than LM hashes

Hybrid Attack

This type of attack depends upon the dictionary attack. There are chances that people might change their password by just adding some numbers to their old password. In this type of attack, the program adds some numbers and symbols to the words from the **dictionary** and tries to **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."

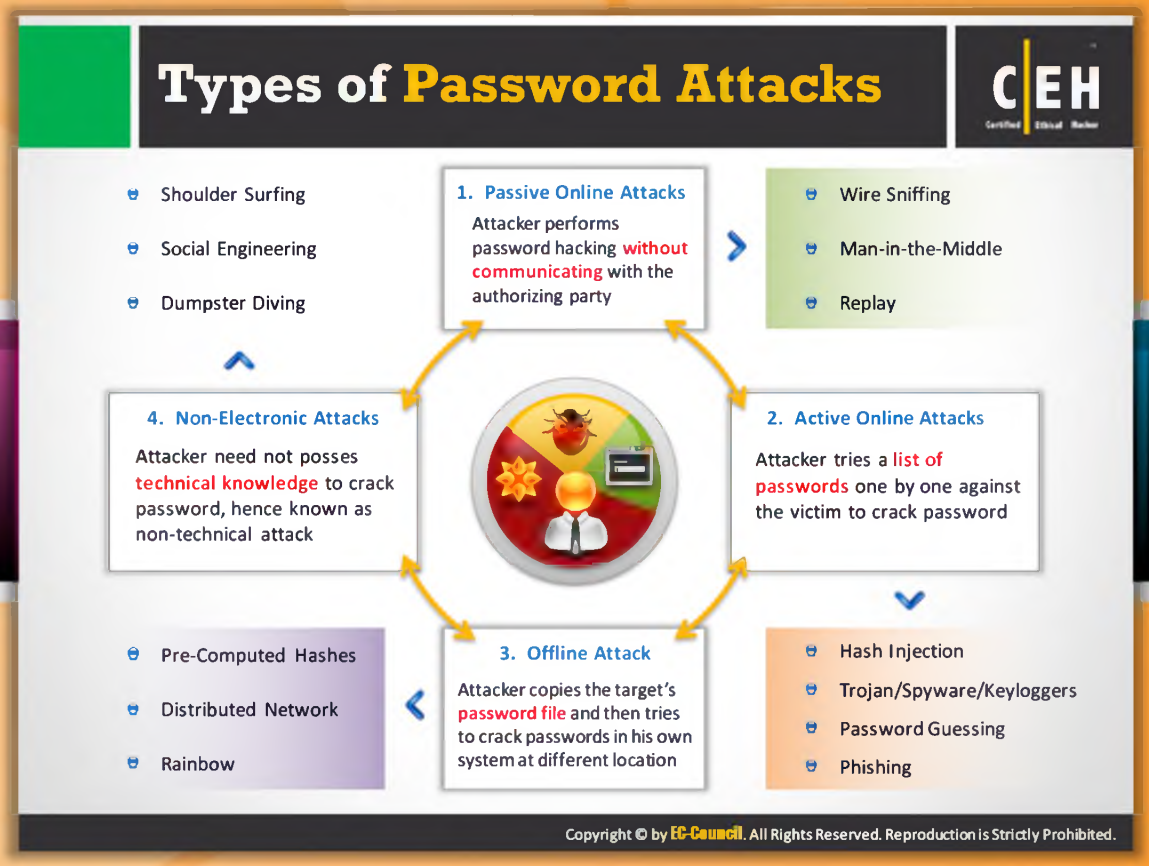
Syllable Attack

A syllable attack is the combination of both a **brute force attack** and the dictionary attack. This **cracking technique** is used when the password is not an existing word. Attackers use the dictionary and other methods to crack it. It also uses the possible **combination** of every word present in the dictionary.

Rule-based Attack

This type of attack is used when the attacker gets some information about the password. This is the most powerful attack because the cracker knows the type of password. For example, if the attacker knows that the password contains a **two-** or **three-digit** number, then he or she will use some **specific techniques** and extract the password in less time.

By obtaining useful information such as use of numbers, the length of password, and special characters, the attacker can easily adjust the time for **retrieving** the password to the minimum and **enhance** the cracking tool to **retrieve passwords**. This **technique** involves brute force, dictionary, and **syllable attacks**.



Types of Password Attacks

Password cracking is one of the crucial stages of **hacking a system**. Password cracking used for **legal** purposes recovers the forgotten password of a user; if it is used by **illegitimate** users, it can cause them to **gain unauthorized privilege** to the network or system. Password attacks are **classified** based on the attacker's actions to crack a password. Usually there are of four types. They are:

Passive Online Attacks

A passive attack is an attack on a system that does not result in a change to the system in any way. The attack is to purely monitor or record data. A **passive attack** on a **cryptosystem** is one in which the **cryptanalyst** cannot interact with any of the parties involved, attempting to break the system solely based upon observed data. There are three types of passive online attacks. They are:

- Wire sniffing
- Man-in-the-middle
- Replay

Active Online Attacks

An active online attack is the easiest way to gain unauthorized **administrator-level** access to the system. There are three types of Active Online Attacks. They are:

- Password guessing
- Trojan/spyware/key logger
- Hash injection
- Phishing

Offline Attacks

Offline attacks occur when the intruder checks the validity of the passwords. He or she observes how the password is stored in the **targeted system**. If the user names and the passwords are stored in a file that is readable, it becomes easy for the **intruder** to **gain access** to the system. In order to protect your passwords list they should always be kept in an unreadable form, which means they have to be **encrypted**.

Offline attacks are often time consuming. They are successful because the **LM hashes** are vulnerable due to a smaller keyspace and shorter length. Different **password cracking techniques** are available on the **Internet**.

The techniques to prevent or protect from offline attacks are:

- Use good passwords
- Remove LM hashes
- Attacker has the password database
- Use cryptographically secure methods while representing the passwords

There are **three types** of offline attacks. They are:

- Pre-computed hashes
- Distributed network
- Rainbow

Non-electronic Attacks

Non-electronic attacks are also known as non-technical attacks. This kind of attack doesn't require any technical knowledge about the methods of **intruding** into another's system. Therefore, it is called a non-electronic attack. There are three types of **non-electronic** attacks. They are:

- Shoulder surfing
- Social engineering
- Dumpster diving

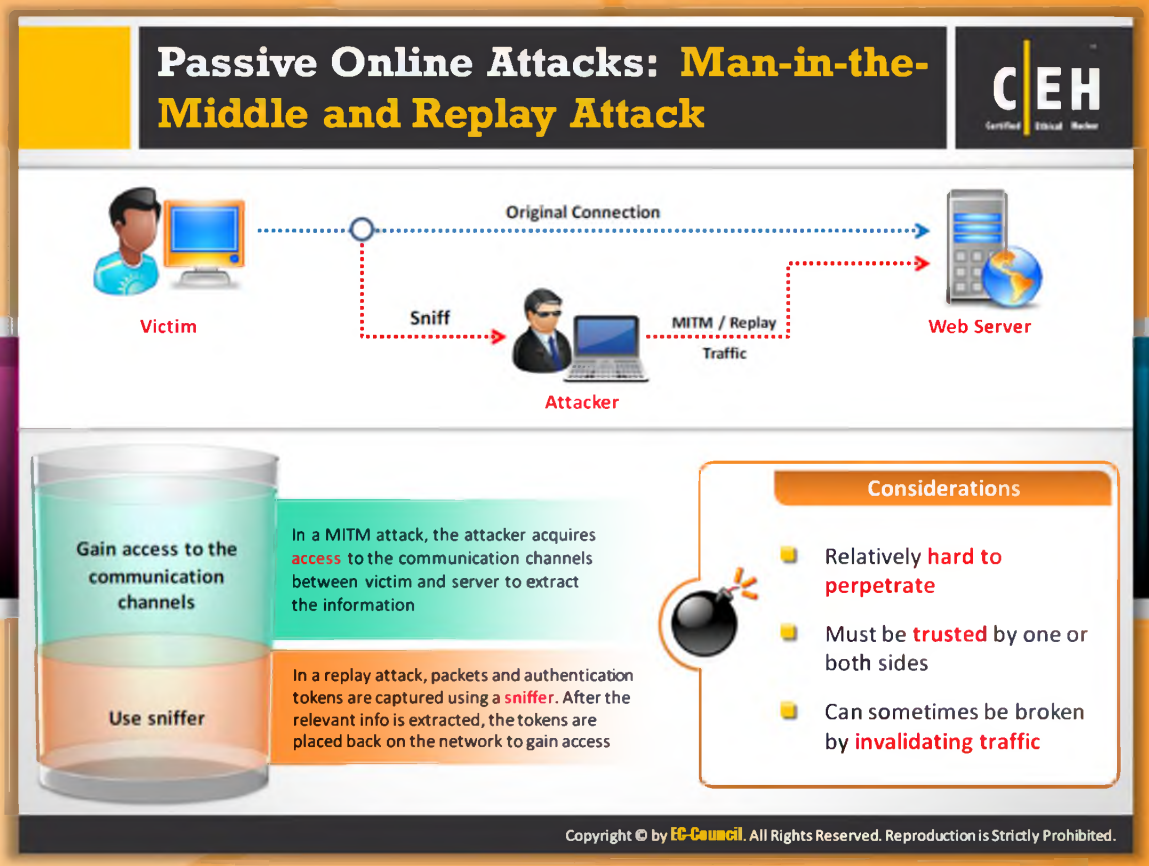
Passive Online Attack: Wire Sniffing

A **packet sniffer tool** is seldom used for an attack. This is because a sniffer can work only in a common collision domain. Common **collision domains** are not connected by a switch or bridge. All the hosts on that network are also not switched or bridged in the network segment.

As sniffers gather packets at the **Data Link Layer**, they can grab all packets on the LAN of the machine that is 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. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. 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 called passive sniffers as they passively wait for data to be sent, 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 **Telnet**, FTP, **rlogin sessions**, and electronic mail sent and received. **Sniffed credentials** are used to gain unauthorized access to the target system. There are a variety of tools available on the Internet for **passive wire sniffing**.

FIGURE 5.3: Passive Online Attack by Using Wire Sniffing

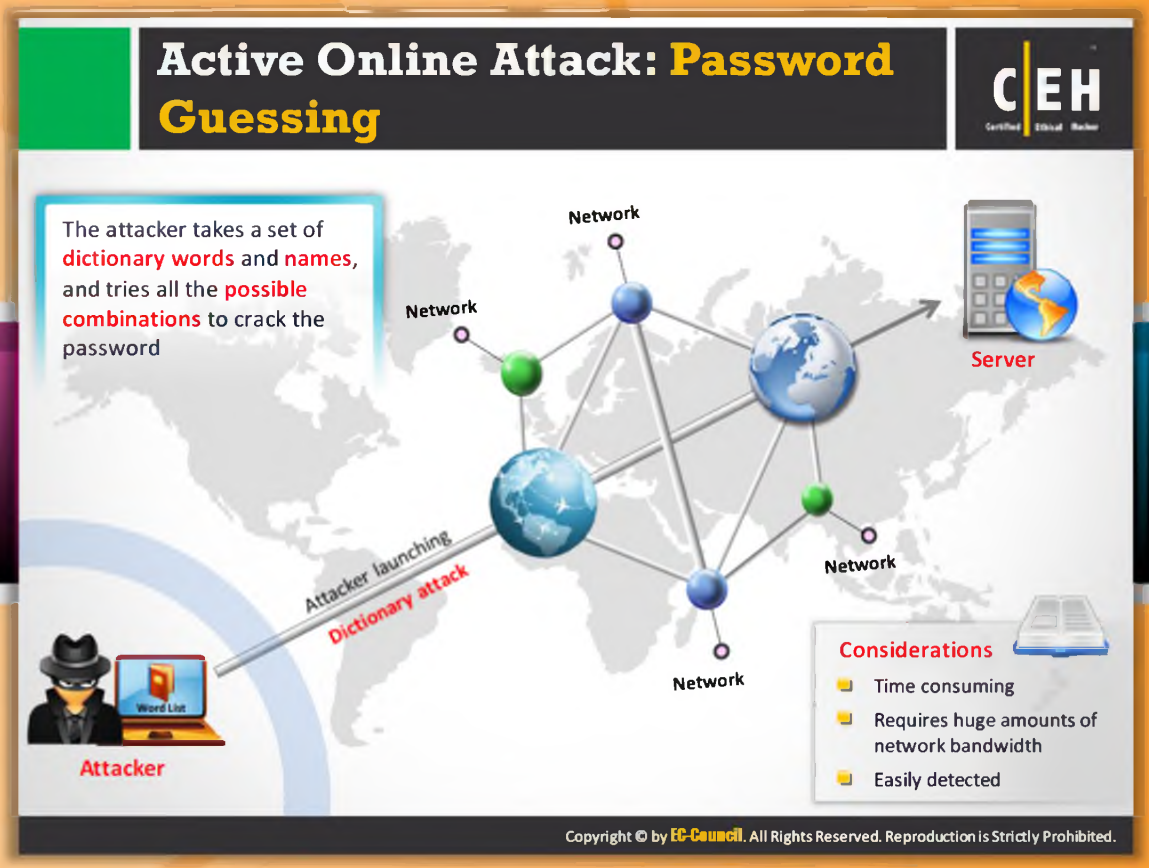


Passive Online Attack: Man-in-the-Middle and Replay Attack

When two parties are communicating, the **man-in-middle attack** can take place. In this case, a third party intercepts the communication between the two parties, assuring the two parties that they are communicating with each other. Meanwhile, the **third party** alters the data or **eavesdrops** and passes the data along. To carry out this, the man in middle has to **sniff** from both sides of the connection simultaneously. This type of attack is often found in telnet and wireless technologies. It is not easy to implement such attacks due to the TCP sequence numbers and speed. This method is relatively hard to **perpetrate** and can be broken sometimes by **invalidating** the traffic.

In a replay attack, packets are captured using a sniffer. After the **relevant** information is extracted, the packets are placed back on the network. This type of attack can be used to replay bank **transactions** or other similar types of data transfer in the hope of **replicating** or **changing** activities, such as deposits or transfers.

FIGURE 5.4: Passive Online Attack by Using Man-in-the-Middle and Replay Attack



Active Online Attack: Password Guessing

Everyone knows your user name, but your password is a well-kept secret in order to keep others away from **accessing your transactions**.

With the aid of dictionary attack **methodologies**, an intruder tries many means to **guess your password**. In this methodology, an attacker takes a set of dictionary words and names, and makes all the possible **combinations** to get your password. The attacker performs this method with programs that guess hundreds or thousands of words per second. This makes it easy for them to try many **variations**: backwards words, different **capitalization**, adding a digit to the end, etc.

To facilitate this further, the attacker community has built large **dictionaries** that include words from foreign languages, or names of things, places, and towns modeled to crack passwords. Attackers can also scan your **profiles** to look for words that might break your password. A good password is easy to remember, but hard to guess, so you need to **protect your password** by making it appear random by inserting such things as digits and **punctuation**. The more **intricate** your password, the more difficult it becomes for the **intruder** to **break**.

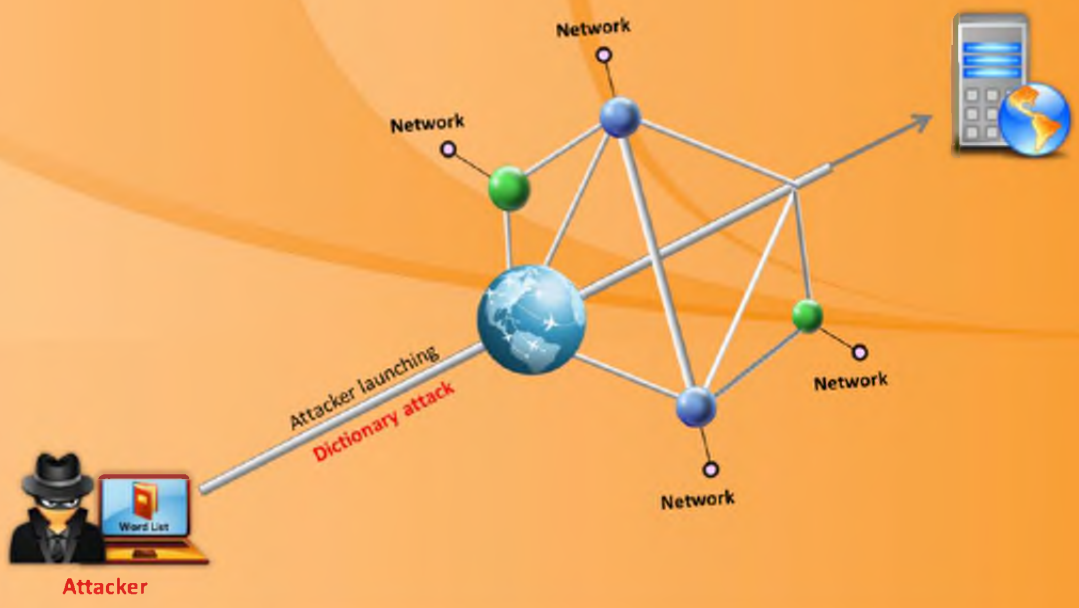
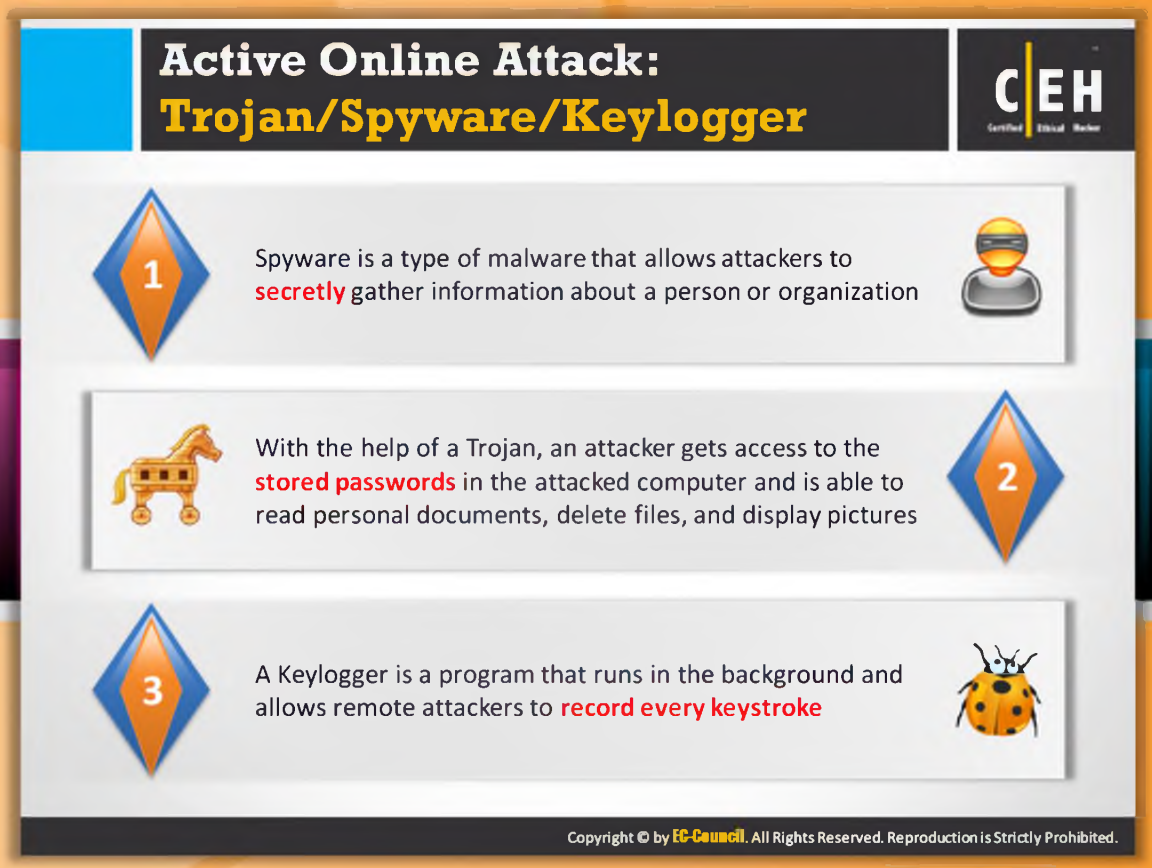


FIGURE 5.5: Active Online Attack by Using Password Guessing Method

Some of the considerations for password guessing are as follows:

- Takes a long time to be guessed
- Requires huge amounts of **network bandwidth**
- It can be easily detected



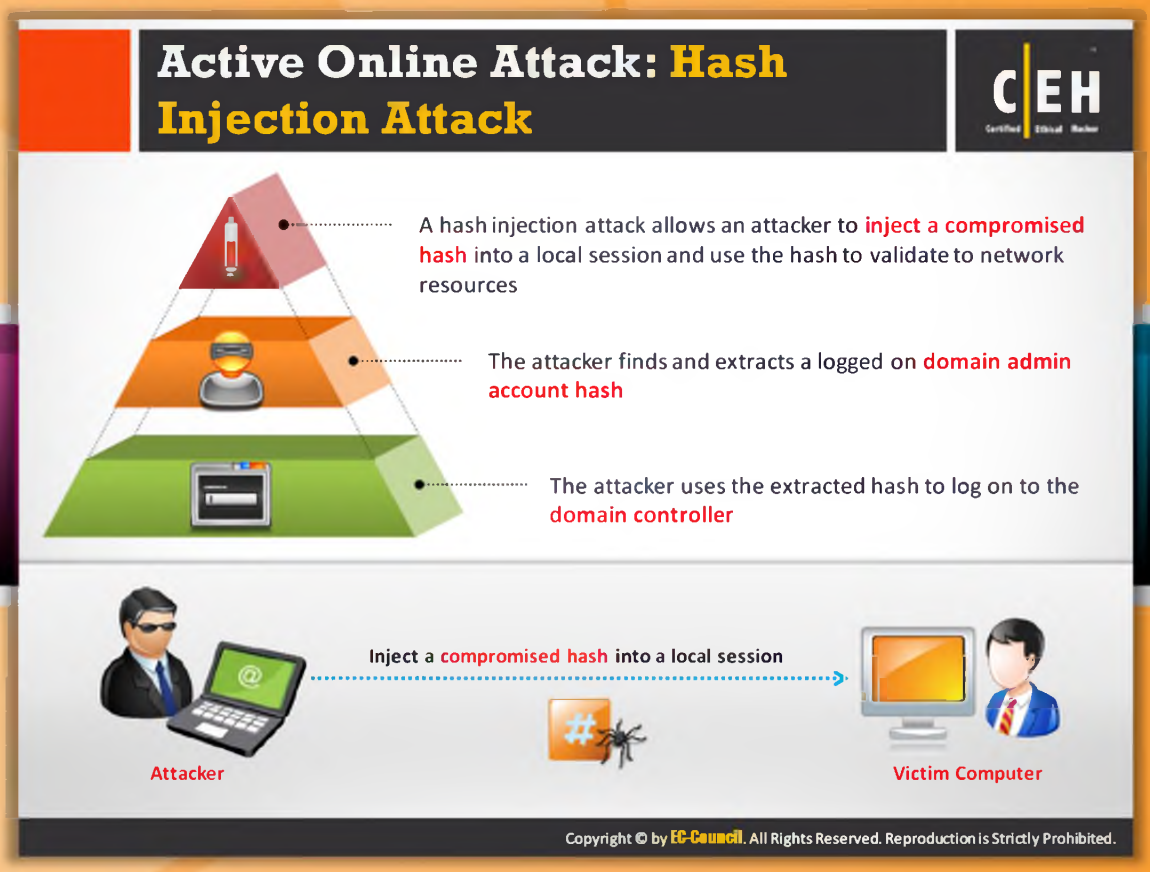
Active Online Attack: Trojan/Spyware/Keylogger

A Trojan is a **destructive** programs that **subterfuge** as a benign application. Prior to the installation and/or execution, the software initially appears to perform a desirable function, but in practice it steals information or harms the system. With a Trojan, attackers may have remote access to the target computer. Attackers can have access to the computer remotely and perform various operations that are limited by user **privileges** on the target computer, by installing the Trojan.

Spyware is a type of **malware** that can be installed on a computer to gather information about the users of the computer without their knowledge. This allows attackers to gather information about the user or the organization secretly. The presence of **spyware** is typically hidden from the user, and can be difficult to detect.

A keylogger is a program that records all the **keystrokes** that are typed on the computer keyboard without the knowledge of the user. Once keystrokes are logged, they are shipped to the attacker, or hidden in the machine for later retrieval. The attacker then **scrutinizes** them carefully for the purpose of finding passwords or other useful information that could be used to compromise the system.

For example, a **keylogger** is capable of **revealing** the contents of all emails composed by the user of the computer system on which the keylogger has been installed.

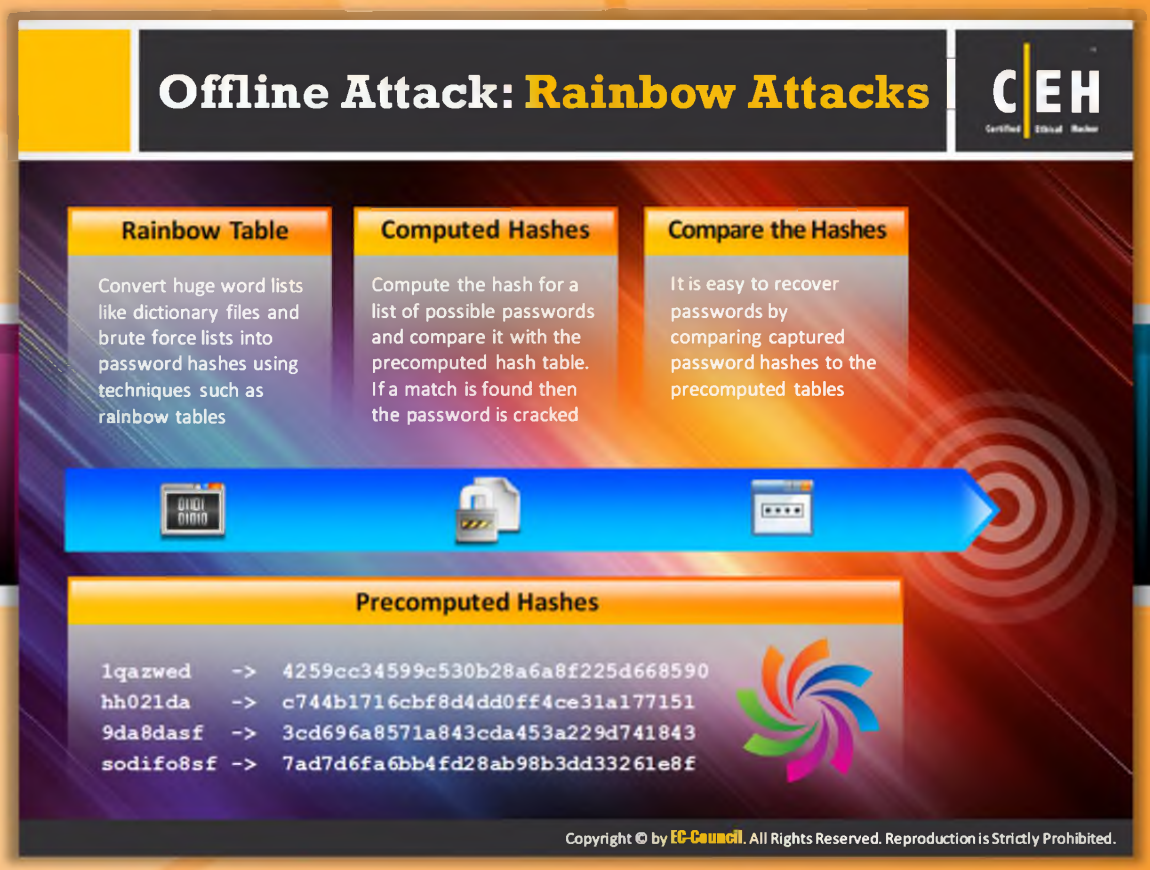


Active Online Attack: Hash Injection Attack

A hash injection attack is the concept of **injecting** a compromised **hash** into a local session and then using the hash to **authenticate** to the network resources. This attack is done successfully in **four steps**. They are:

- The hacker compromises one workstation/server using a local/remote exploit
- The hacker extracts logged-on hashes and finds a logged-on domain admin account hash
- The hackers use the hash to log on the **domain controller**
- The hacker extracts all the hashes in the **Active Directory database** and can now **satirize** any account in the domain

FIGURE 5.6: Active Online Attack by Using Hash Injection Attack



Offline Attack: Rainbow Attacks

Offline attacks occur when the intruder checks the **validity** of the **passwords**. He or she observes how the password is stored. If the user names and the passwords are stored in a file that is **readable**, it becomes easy for him or her to gain access to the system. Hence, the passwords list must be protected and kept in an unreadable form, such as an **encrypted** form.

Offline attacks are time consuming. They are successful because the **LM hashes** are vulnerable due to smaller **keyspace** and shorter length. Different password **cracking techniques** are available on the Internet.

There are two types of offline attacks that an attacker can perform to discover the password.

- Rainbow Attacks
- Distributed network Attacks

Rainbow Attacks

A rainbow attack is the implementation of the **cryptanalytic time-memory** trade-off technique. Cryptanalytic time-memory **trade-off** is the method that requires less time for cryptanalysis. It uses already calculated information stored in the memory to crack the cryptography. In the

rainbow attack, the same technique is used; the password hash table is created in advance and stored into the memory. Such a table is called a "rainbow table."

Rainbow Table

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

Computed Hashes

An attacker computes the hash for a list of possible passwords and compares it with **the pre-computed** hash table (rainbow table). If a match is found, then the password is **cracked**.

Compare the Hashes

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

Pre-Computed Hashes

Only encrypted passwords should be stored in a file containing user **name/encrypted password pairs.** The typed password is encrypted using the hash function of cryptography during the **logon process**, and it is then compared with the password that is stored in the file.

Encrypted passwords that are stored can prove useless against **dictionary attacks**. If the file that contains the encrypted password is in a readable format, the attacker can easily detect the hash function. He or she can then decrypt each word in the dictionary using the hash function, and then compare with the encrypted password. Thus the **attacker obtains** all passwords that are words listed in the dictionary.

Storage of hashes requires large memory space such as LM "hashes" require 310 Terabytes and NT Hashes < 15 chars requires 5,652,897,009 **Exabytes**. Use a time-space tradeoff technique to reduce memory space required to store hashes.

```
1qazwed    ->  4259cc34599c530b28a6a8f225d668590
hh021da    ->  c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf   ->  3cd696a8571a843cda453a229d741843
sodifo8sf  ->  7ad7d6fa6bb4fd28ab98b3dd33261e8f
```

Tools to Create Rainbow Tables: Winrtgen and rtgen

Attackers can create **rainbow tables** by using following tools.

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. It supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384), and SHA-2 (512) hashes.

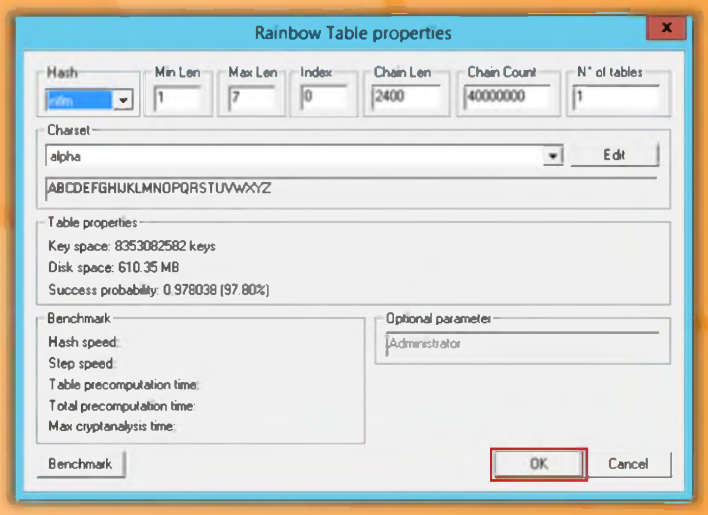


FIGURE 5.7: Winrtgen Generate Rainbow Table in Window

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 is used to generate the rainbow tables. The rtgen program needs several parameters to generate a rainbow table; you can use following **syntax** of the command line to generate rainbow tables:

Syntax: rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index

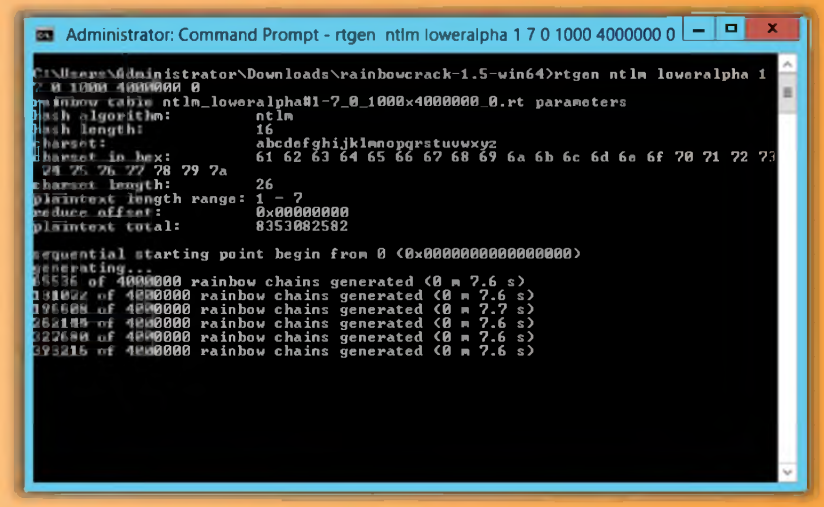
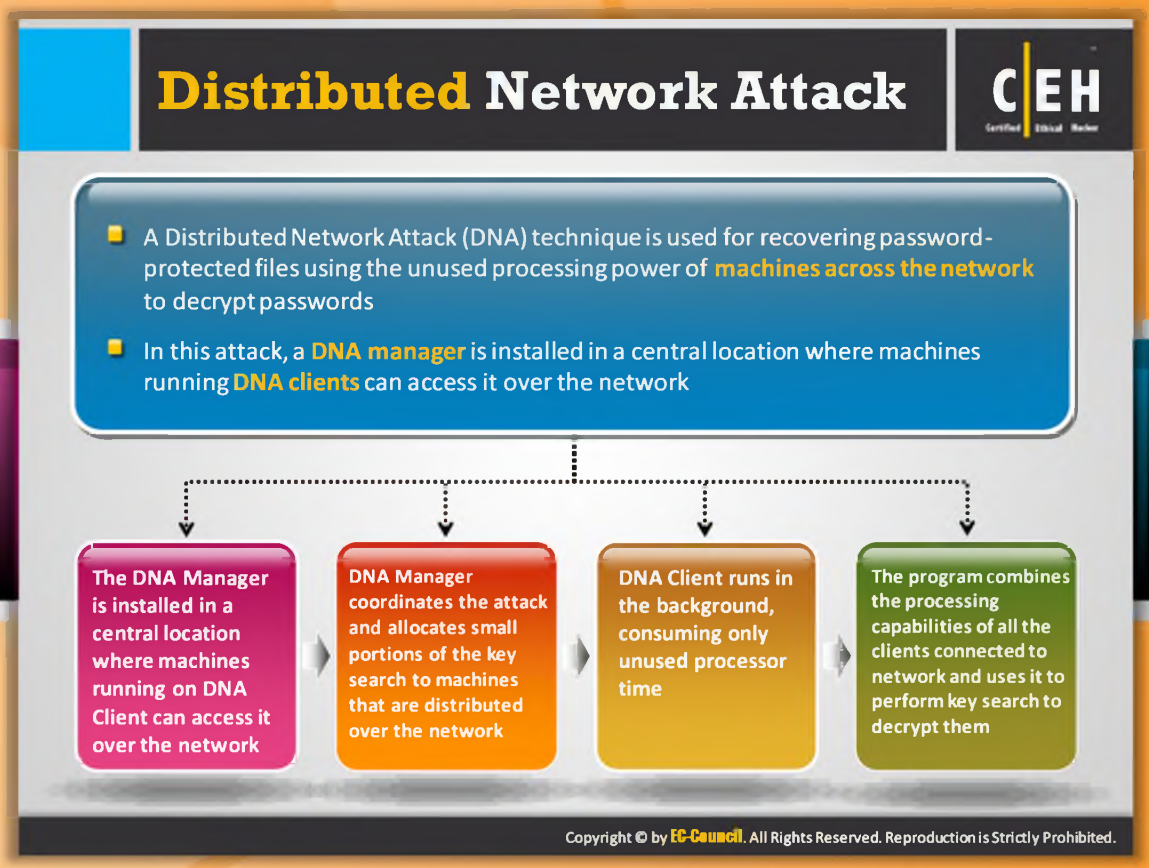


FIGURE 5.8: rtgen Generate Rainbow Table in Window



Distributed Network Attacks

A Distributed Network Attack (DNA) is the technique used for **recovering password-protected files.** It utilizes the unused processing power of machines across the network to decrypt passwords. In this attack, a DNA manager is installed in a central location where machines running DNA clients can access it over the 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 network and uses them to perform a key search on Office 97 and 2000 to **decrypt** them.

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 of stealth client installation functionality
- Automatically updates client while updating the DNA server

- Controls the clients and identifies work done by clients

DNA is divided 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 is divided into:

- **Current jobs**: The current job queue has all the jobs that have been added to the list by the controller. The current job list has many columns, such as the **identification number** that has been assigned by the DNA to the job, the name of the encrypted file, the password that has been used by the user, the password that matches a key which can unlock data, the status of the job, and various other columns.
- **Finished jobs:** The finished job list provides information about the jobs that can be decrypted by including the password. The finished jobs 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**, etc.

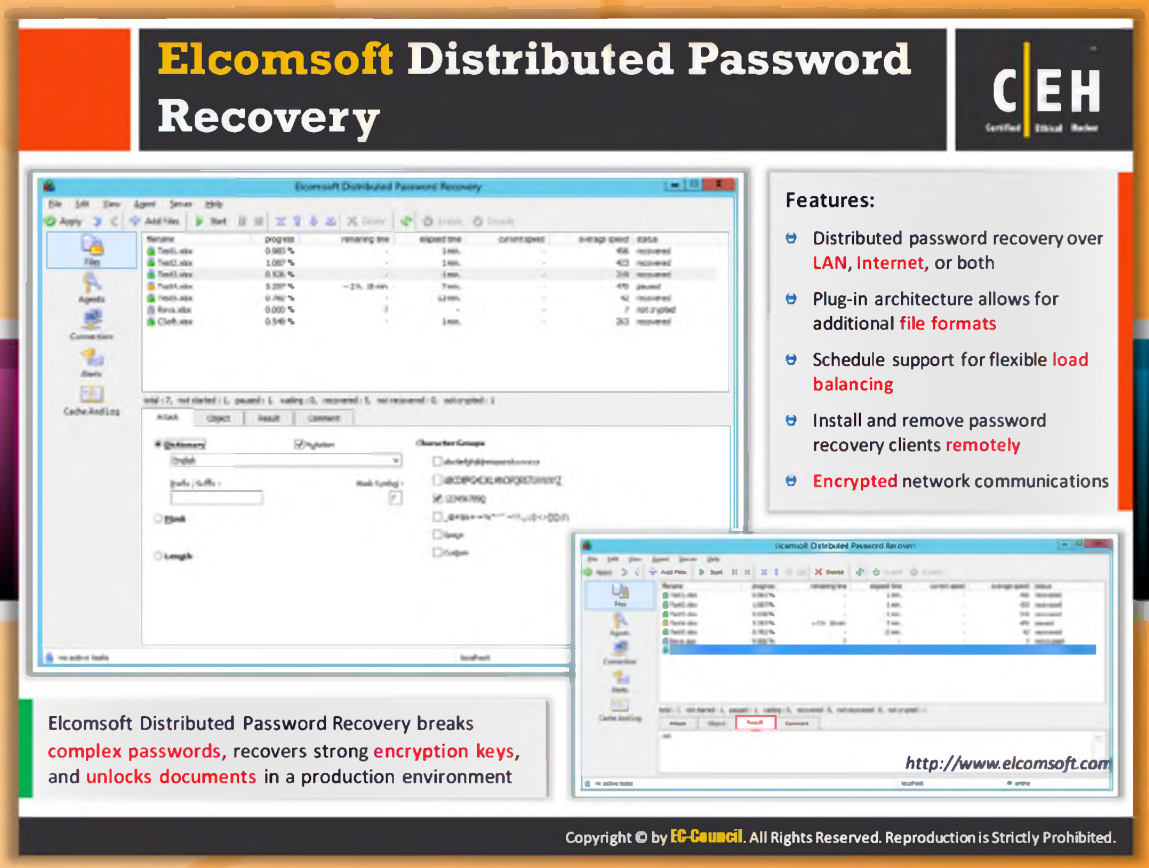
DNA Client Interface

The DNA client interface can be used from many workstations. The **client statistics** can be easily coordinated by using the DNA client interface. This interface is available on machines where the DNA client application has been installed. 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 application in Windows is used for the purpose of network management. The Network Traffic dialog box is used to find out the network speed that 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. When the data is collected from the Network Traffic dialog box, **modification** to the client work unit can be made. When the size of the work unit length increases, the speed of the network traffic decreases. If the traffic has been decreased, the client work on the jobs would require a **longer amount of time**. Therefore, fewer requests to the server can be made due to the reduction in the **bandwidth** of network traffic.



Elcomsoft Distributed Password Recovery

Source: http://www.elcomsoft.com

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

Features & Benefits

- Reduces password recovery time
- Distributed password recovery over LAN, Internet, or both
- **Solace management** for **flexible control** from any networked PC
- Plug-in **architecture** allows for additional file formats
- Flexible queue control allows easy job management
- Install and remove password recovery clients remotely

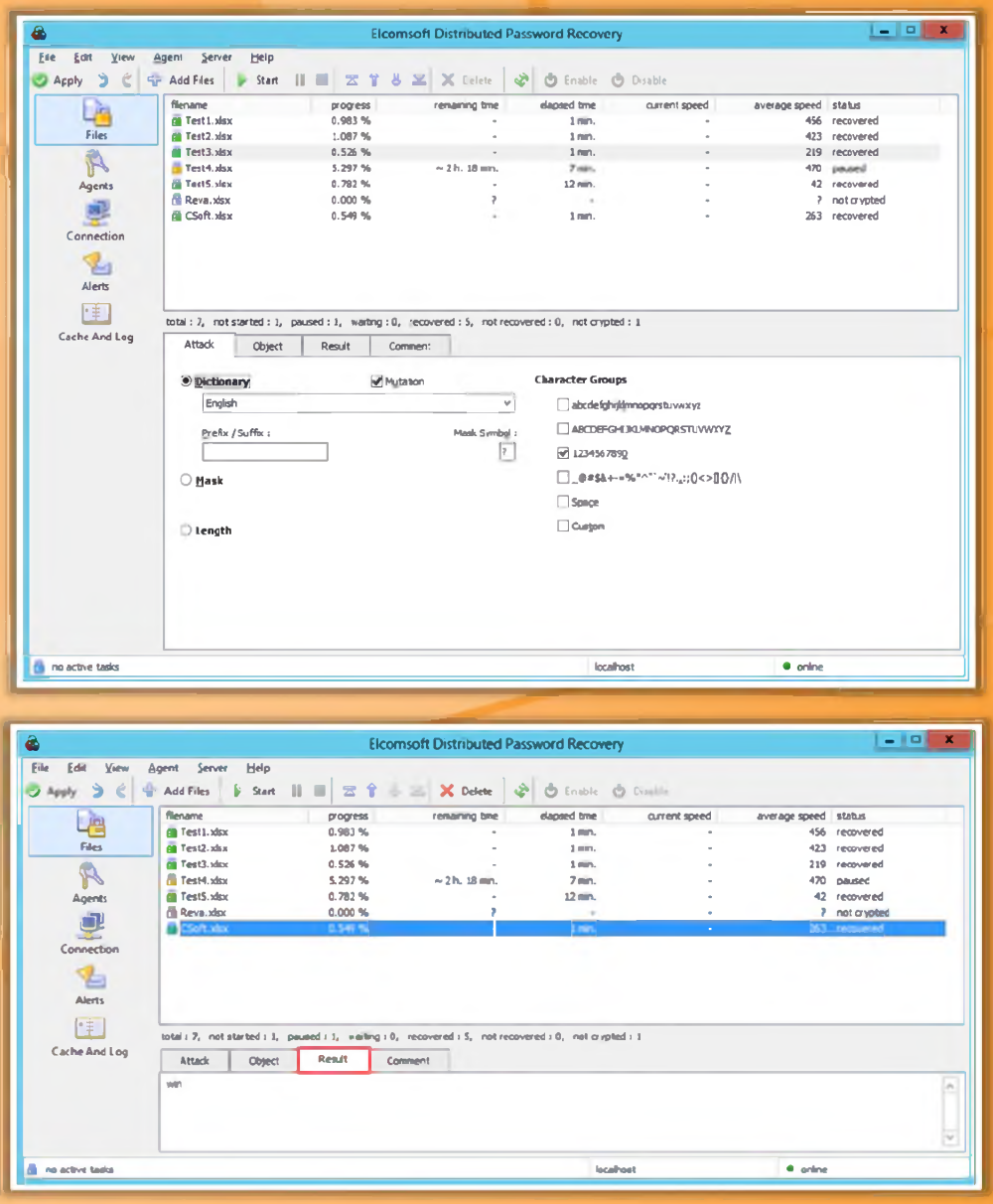
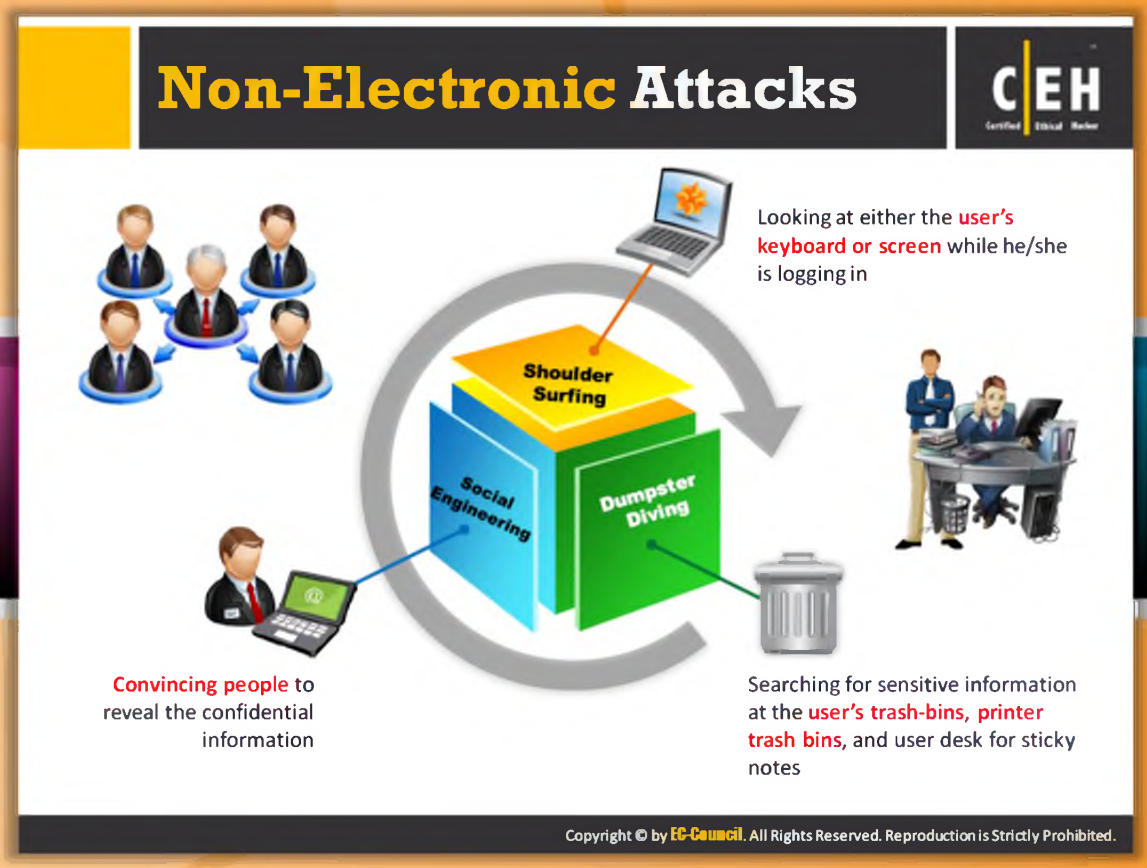


FIGURE 5.9: Elcomsoft Distributed Password Recovery Screenshot



Non-Electronic Attacks

Non-electronic attacks are also termed **non-technical attacks**. This kind of attack doesn't require any **technical knowledge** about the methods of intruding into another's system. Therefore, it is named a non-electronic attack. There are four types of non-electronic attacks, which are: social engineering, shoulder surfing, keyboard sniffing, and dumpster diving.

Dumpster Diving

Dumpster diving is a key attack method that targets upon a **substantial failure** in computer security: the very information that people crave, protect, and devotedly secure can be attained by almost anyone willing to **scrutinize** garbage. It allows you to gather information about the target's passwords by looking through the trash. This low-tech attack type has many implications.

Due to less security than there is today, dumpster diving was actually quite popular in the 1980s. The term "dumpster diving" refers to any useful, general information that is found and taken from areas where it has been **discarded**. These areas include trash cans, curbside containers, dumpsters, and the like, from which the information can be obtained for free. Curious and/or malicious attackers may find password files, manuals, sensitive documents, reports, receipts, credit card numbers, or **diskettes** that have been thrown away.

Simply, the examination of waste products that have been dumped into the dumpster areas may be helpful to attackers, and there is ample information to support this concept. Such useful information was dumped with no thought to whose hands it may end up in. This data can be utilized by the attackers to gain unauthorized access on others' computer systems, or the objects found can prompt other types of attacks such as those based on social engineering.

Shoulder Surfing

Shoulder surfing is when an intruder is standing inconspicuously, but near a legitimate user, watching as the password is entered. The attacker simply looks at either the user's keyboard or screen while he or she is logging in, and watches to see if the user is staring at the desk for a password reminder or the actual password. This can be possible only when the attacker is physically close 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. Many of these Personal Identification Numbers are only four digits long.

Eavesdropping refers to the act of secretly listening to someone's conversation. Passwords can be determined by secretly listening to the password exchanges. If the hacker fails to get your password by guessing, there are other ways he or she can try to get it. "Password sniffing" is an alternative used by the hackers to get their target passwords.

Most of the networks use broadcast technology, which means that every message that a computer on the network transmits can be read by each and every computer connected on that network. In practice, except the recipient of the message, all other computers will notice that the message is not intended for them, and ignore it.

However, computers can be programmed to look at every message transmitted by a specific computer on the network. In this way, one can look at messages that are not intended for them. Hackers have the programs to do this, and then scan all the messages traversed on the network looking for the password.

You may end up giving your password to the attacker if you are logging into a computer across a network, and some computers on the network have been compromised this way.

Using this password sniffing technique, hackers have collected thousands of passwords by breaking into the computers that are connected on a heavily used network.

Social Engineering

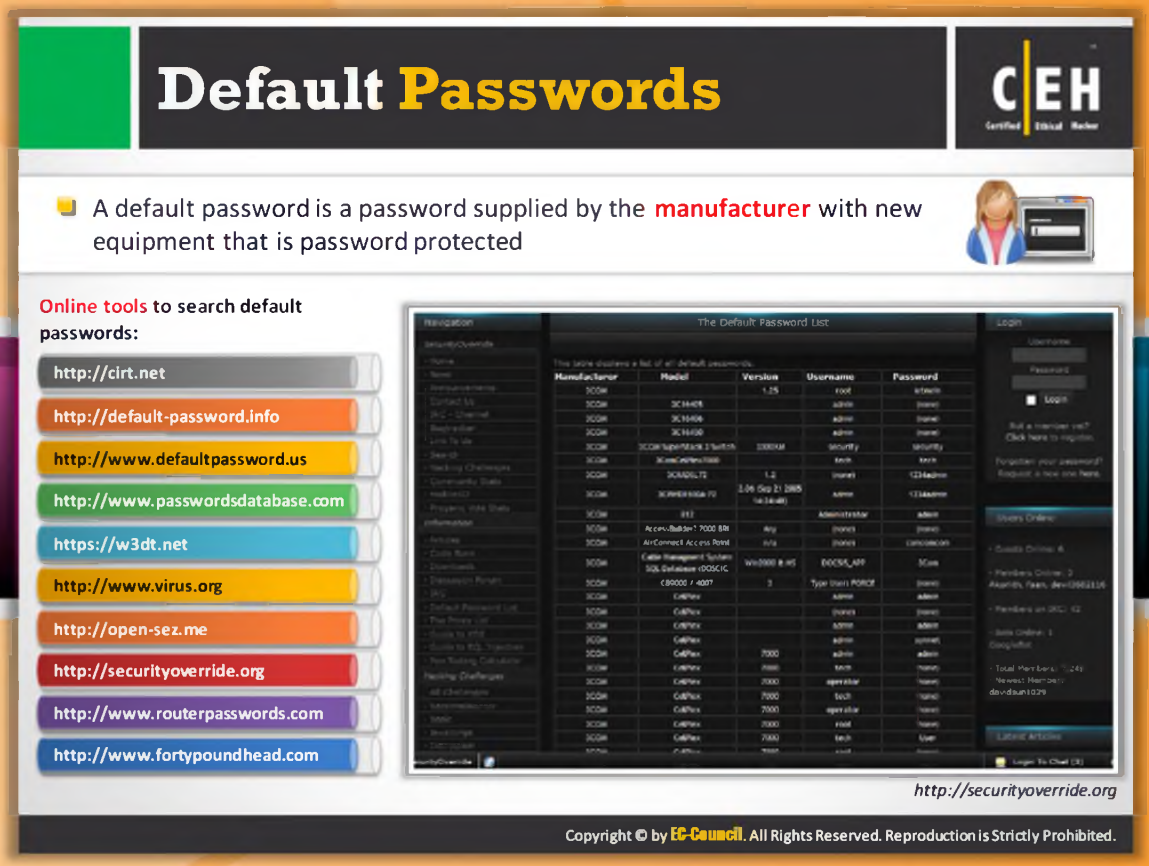
In computer security, social engineering is the term that represents a non-technical kind of intrusion. Typically, this relies heavily on human interaction and often involves tricking other people into breaking normal security procedures. A social engineer runs a "con game" to break the security procedures. For example, an attacker using social engineering to break into a computer network would try to gain the trust of someone who is authorized to access the network, and then try to extract the information that compromises the network security.

Social engineering is the run-through of procuring **confidential information** by deceiving or swaying people. An attacker can **misrepresent** himself as a user or system administrator in order to obtain the password from a user. It is natural for people to be helpful and **trusting**. Any person generally makes an effort to build **amicable** relationships with his or her 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 careless about protecting it. Attackers take advantage of this fact for the intrusion. Habitually, social engineers search **dumpsters** for valuable information. A social engineer would have a tougher time getting the combination to a safe, or even the combination to a health **club locker**, than a password. The best **defense** is to educate, train, and create awareness.

Keyboard Sniffing

Keyboard sniffing allows you to interpret the password as the target enters the keystrokes using **keyloggers**.



Default Passwords

Source: http://securityoverride.org

Default passwords are passwords supplied by **manufacturers** with new equipment. Usually the default password provided by the manufacturers for password protected devices allows the device to be accessed during its initial setup. **Online tools** that can be used to search for default passwords include:

- http://cirt.net
- http://default-password.info
- http://www.defaultpassword.us
- http://www.passwordsdatabase.com
- https://w3dt.net
- http://www.virus.org
- http://open-sez.me
- http://securityoverride.org
- http://www.routerpasswords.com
- http://www.fortypoundhead.com

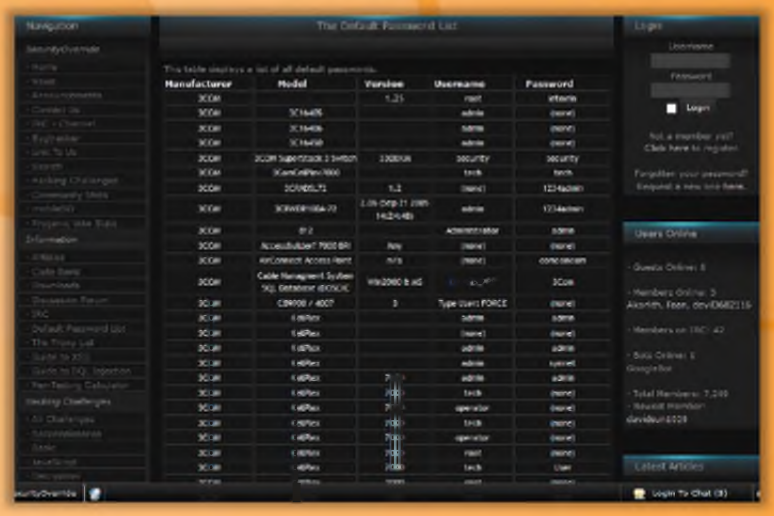
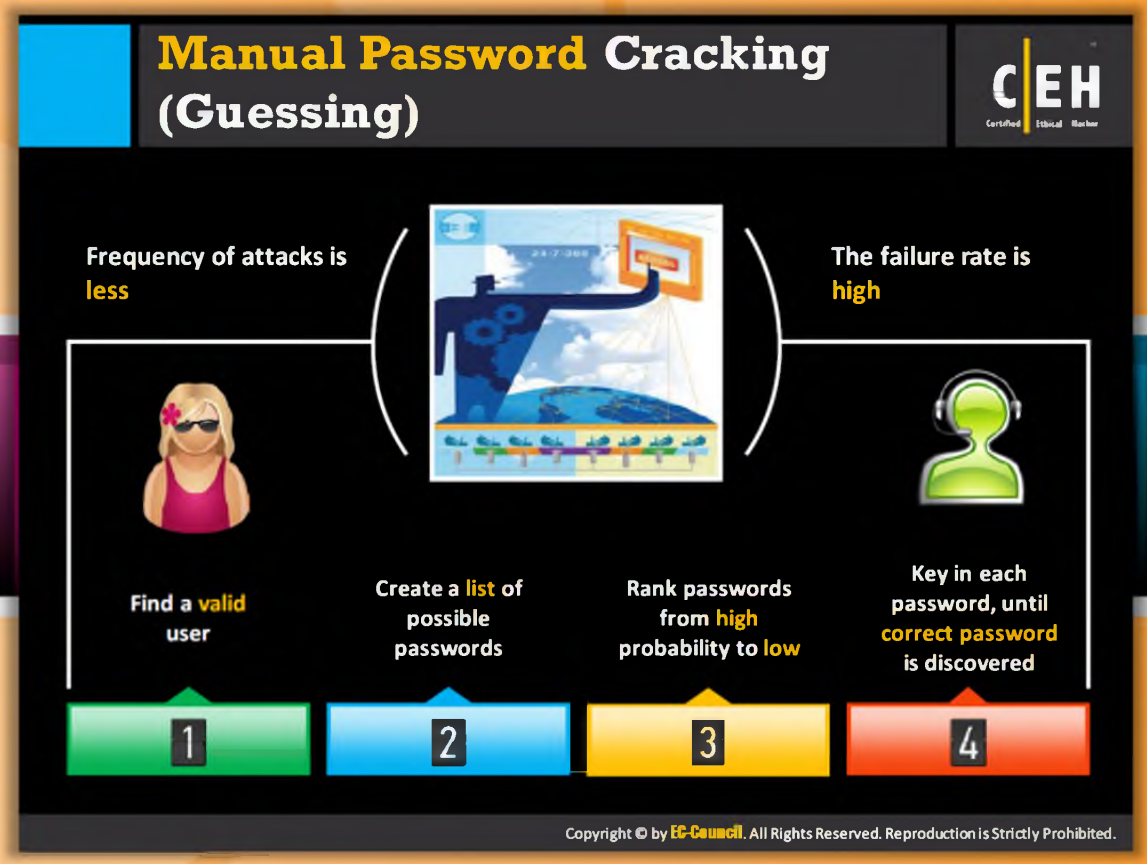


FIGURE 5.10: Default Password Screenshot

Vendor	Model	Version	Access Type	User-name	Password
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Debug	Synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Tech	Tech
3COM	HiPerARC	v4.1.x	Telnet	Adm	(none)
3COM	LANplex	2500	Telnet	Debug	Synnet
3COM	LANplex	2500	Telnet	Tech	Tech
3COM	LinkSwitch	2000/2700	Telnet	Tech	Tech
Huawei	E960			Admin	Admin
3COM	NetBuilder		SNMP		ILMI
3COM	Netbuilder		Multi	Admin	(none)
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3COM	SuperStack II Switch	2200	Telnet	debug	Synnet
3COM	SuperStack II Switch	2700	Telnet	tech	Tech
3COM	OfficeConnect 812 ADSL		Multi	adminttd	adminttd

TABLE 5.1: Online Tools To Search Default Password



Manual Password Cracking (Guessing)

Manual password cracking **encompasses** attempting to log on with different passwords. Guessing is the key element of manual password cracking. The password is the key value of data that is needed to access the system. Most passwords can be cracked using different **escalation privileges**, executing applications, hiding files, and covering tracks. Attackers try many attempts to crack passwords to intrude into a target's system. Passwords can be cracked manually or using some **automated tools**, methods, and **algorithms**. Password cracking can be automated using a simple FOR loop also. Manual password cracking involves different attempts to log in the following ways:

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

A hacker can also create a script file that tries each password in a list. Still this is still considered manual cracking. The failure rate of this type of attack is high.

Manual Password Cracking Algorithm

In its simplest form, password guessing can be automated using a simple FOR loop. In the example that follows, an attacker creates a simple text file with user names and passwords that are iterated using the **FOR loop**.

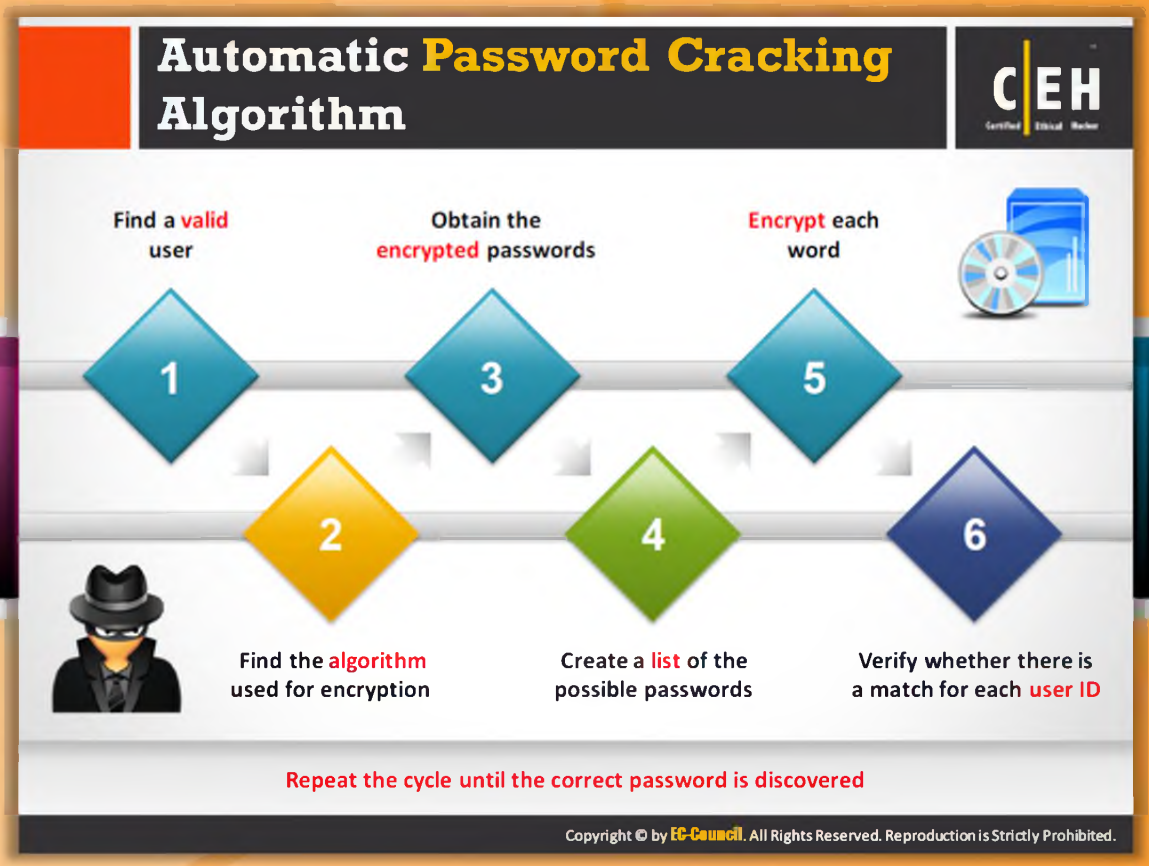
The main FOR loop can extract the user names and passwords from the **text file** that serves as a dictionary as it iterates through every line:

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

From a directory that can access the text file, the command is typed as follows:

```
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 **open session** can be established with the **victim server** using the attacker's system.



Automatic Password Cracking Algorithm

As security awareness increased, most systems began running passwords through some type of **algorithm** to generate a hash. This hash is usually more than just **rearranging** the original password. It is usually a **one-way hash**. The one-way hash is a string of characters that cannot be reversed into its original text.

However, the vulnerability does not arise from the hashing process, but from password storage. The password that is stored at the time of **authentication** is not **decrypted** by most of the systems. Such systems store only one-way hashes.

During the local login process, the password entered is run through the algorithm generating a one-way hash and **comparing** it to the hash stored on the system. If they are found to be similar, it is assumed that the proper password was used.

Therefore, all that an attacker has to do in order to crack a password is to get a copy of the one-way hash stored on the server, and then use the algorithm to generate his or her own hash until he or she gets a match. Most **systems—Microsoft**, UNIX, and Netware—have publicly announced their **hashing algorithms**.

Attackers can use a **combination of attack** methods to reduce the time involved in cracking a password. The Internet provides freeware password crackers for NT, Netware, and UNIX.

There are password lists that can be fed to these crackers to carry out a **dictionary attack**. In its simplest form, **automation** involves finding a valid user and the particular **encryption algorithm** being used, obtaining encrypted passwords, creating a list of all possible passwords, encrypting each word, and checking for a match for each user ID known. This process is repeated until the desired results are obtained or all options are **exhausted**.

Automatic password cracking algorithms should include the following steps:

- Find a valid user
- Find encryption algorithm used
- Obtain encrypted passwords
- Create a list of possible passwords
- Encrypt each word
- See if there is a match for each user ID

Performing Automated Password Guessing

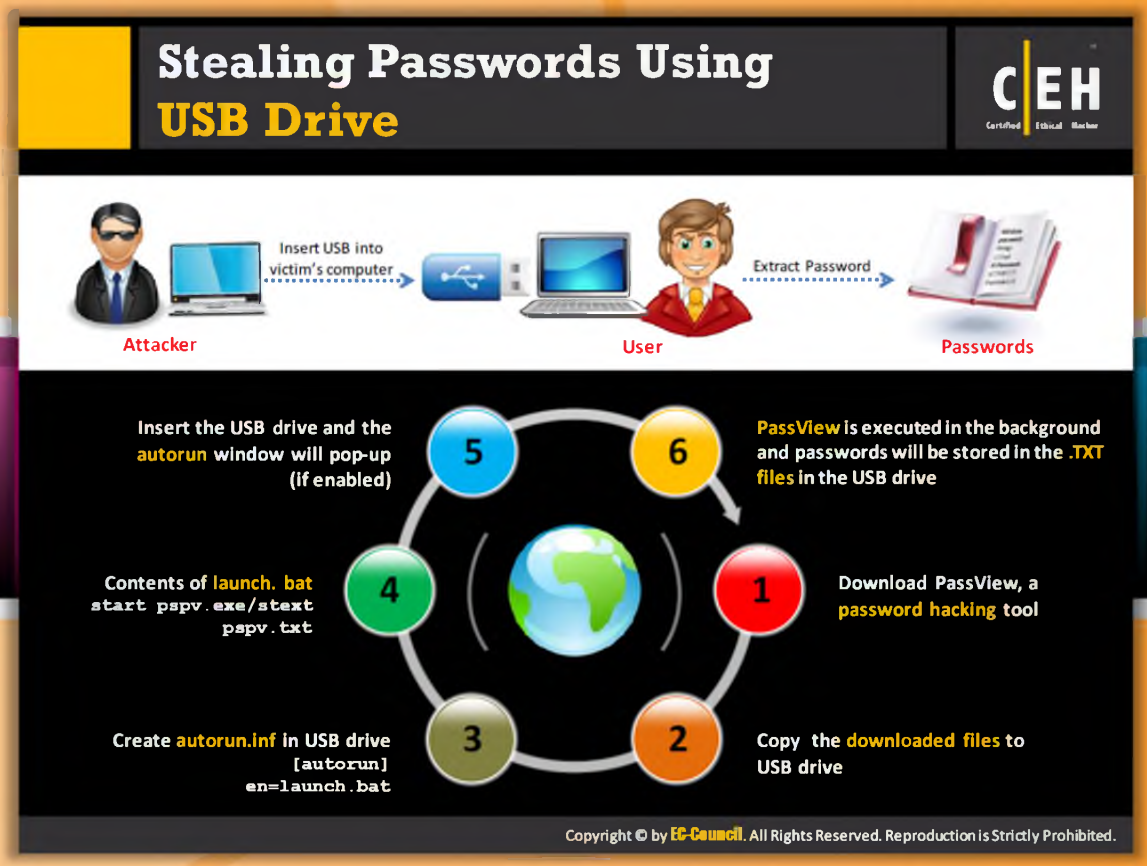
If the attacker fails in a **manual attack**, he or she can choose to **automate** the process. There are several free programs that can assist in this effort. Some of these free programs are Legion, Jack the Ripper, NetBIOS **Auditing Tool** (NAT), etc. The simplest of these **automation** methods take advantage of the net command. This involves a simple loop using the NT/2000 shell for command. All the attacker has to do is to create a simple user name and password file. He or she can then reference this file within a **FOR command**.

```
C:\> FOR /F "token=1, 2*" %i in (credentials.txt)
do net use \\target\IPC$ %i /u: %j
```

Automated password attacks can be categorized as follows:

- A simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as **L0phtCrack** or **John the Ripper**, and running it against user accounts that the application locates. Dictionary attacks are more effective with long words.
- The brute force method is the most inclusive, although slow. Usually it tries every possible letter and number combination in its **automated exploration**.
- A hybrid approach is one that combines features of both methods. It usually starts with a dictionary, and then tries combinations such as two words together or a word and numbers.

Users tend to have weak passwords because they do not know what constitutes a strong password and, therefore, do not know how to create **strong passwords** for their accounts. As shown, this leaves passwords open to attack.



Stealing Passwords Using USB Drives

Stealing passwords using a **USB drive** is a physical approach for hacking passwords stored in a computer. 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 to use if 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 in any computer. Most of the people signing up for a large number of websites usually store their passwords on the computer in order to remember them. One can try recovering them automatically using a USB drive. This requires plugging the **USB** in any port of the computer in which the passwords have been stored. This trick is applicable for Windows XP, Windows 7, Windows Vista, and Windows 2000.

All the applications included are portable and light enough that they can be downloaded in the USB disk in few seconds. You can also hack stored **Messenger passwords**. Using tools and a USB pendrive you can create a rootkit to hack passwords from the target computer.

Stealing passwords using a USB device is carried out with the help of the following steps:

1. You need a password hacking tool

2. Copy the downloaded .exe files of password hacking tools to USB drive.
3. Create a notepad document and put the following content or code in the notepad

   [autorun]

   en=launch.bat

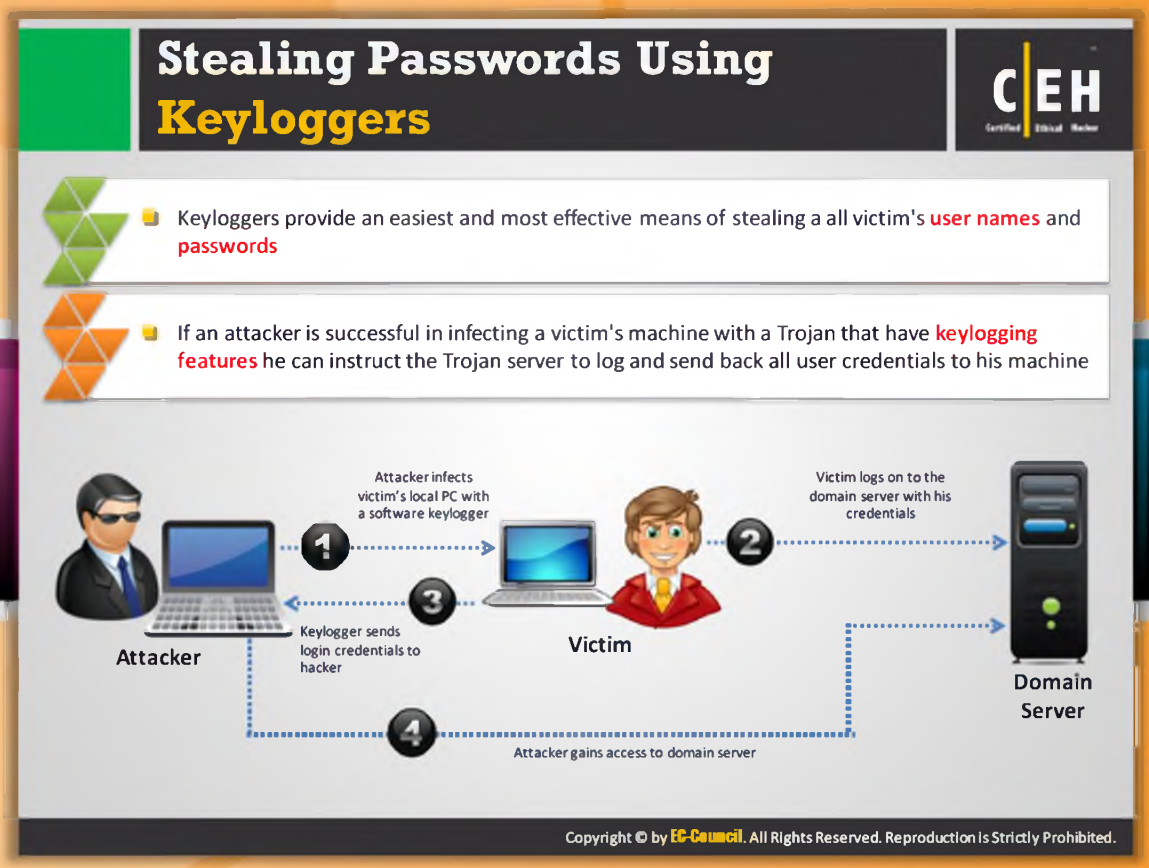
   After writing this content into Notepad, save the document as autorun.inf and copy this file to the USB drive.
4. Open **Notepad** and write the following content into Notepad:

   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 (if enabled).
6. A **password-hacking** tool is executed in the background and passwords can be stored in the .TXT files in 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 the **knowledge** of the person. This process takes only a few seconds to **retrieve** passwords.

FIGURE 5.11: Stealing Passwords Using USB Drives



Stealing Passwords Using Keyloggers

Whenever an attacker needs to crack something, he or she usually thinks about the possible loopholes in the whole process. Passwords are the piece of data used to access an account or a system. Choosing complex passwords makes your accounts secure and the job of the attacker difficult. A complex password makes the attacker's job difficult but not impossible. Passwords are the piece of data to be submitted to a system or application to gain access to it. Passwords are usually entered through the keyboard. Hence, if an attacker has software or a mechanism that can log the keystrokes and send the report to him or her, then the attacker can determine the passwords easily. The programs that allow them to do this are keyloggers, a kind of malware. Keyloggers can expose all the keystrokes entered by the target including user names and passwords for any websites. A remote keylogger can give an attacker access not only to your email and online accounts, but it can compromise your financial details as well. Keyloggers are used by people to find a certain piece of information such as a user name or password. The pictorial representation clearly explains the way attackers steal passwords using keyloggers.

FIGURE 5.12: Stealing Passwords Using Keyloggers

When stealing passwords, the attacker first infects the victim's local PC with a software keylogger. When the victim logs on to the domain server with his or her credentials, the keylogger automatically sends login credentials (user name, passwords) to the attacker without the knowledge of the victim. Once the attacker gets the victim's login credentials, he or she logs on to the domain server and may perform any action.

Microsoft Authentication

SAM Database

The acronym SAM database is the Security Accounts Manager database. This is used by Windows to manage user accounts and passwords in the hashed format (one-way hash). Passwords are never stored in plaintext format. They are stored in the hashed format to protect them from attacks. The **SAM database** is implemented as a **registry file** and the Windows kernel obtains and keeps an exclusive filesystem lock on the SAM file. As this file is provided with a filesystem lock, this provides some measure of security for the storage of the passwords.

It is not possible to copy the SAM file to another location in the case of online attacks. Since the SAM file is locked with an exclusive **filesystem** lock, it cannot be copied or moved while Windows is running. The lock will not release until the blue screen **exception** has been thrown or operating system has shut down. However, making the password **hashes** available for offline **brute-force attacks**, the on-disk copy of the contents of the SAM file can be dumped using various techniques.

Microsoft introduced the **SYSKEY function** in Windows NT 4.0 in an attempt to improve the security of the SAM database against offline software **cracking**. The on-disk copy of the SAM file

is partially encrypted when the SYSKEY is enabled. In this way the password hash values for all local accounts stored in the SAM are encrypted with a key.

Even if its contents were discovered by some subterfuge, the keys are encrypted with a one-way hash, making it difficult to break. Also, some versions have a **secondary key**, making the encryption specific to that copy of the OS.

NTLM Authentication

NTLM (NT LAN Manager) is a proprietary protocol employed by many Microsoft products to perform challenge/response authentication, and it is the default authentication scheme that Microsoft firewall and proxy server products use. This software was developed to address the problem of working with Java technologies in a Microsoft-oriented environment. Since 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.

NTLM Authentication Protocol

Products that are supported by NTML protocol are published only by Microsoft due to the unavailability of the official protocol specifications.

As a consequence, in a Microsoft-oriented network environment, nearly all non-MS products have trouble performing their tasks correctly. Software development environments suffer from the aforementioned problem; there are no libraries that implement this authentication scheme, except the ones bundled in the Windows OS. In the Open Source community, there are many projects focused on the implementation of this protocol, but most of these have Java as the target environment.

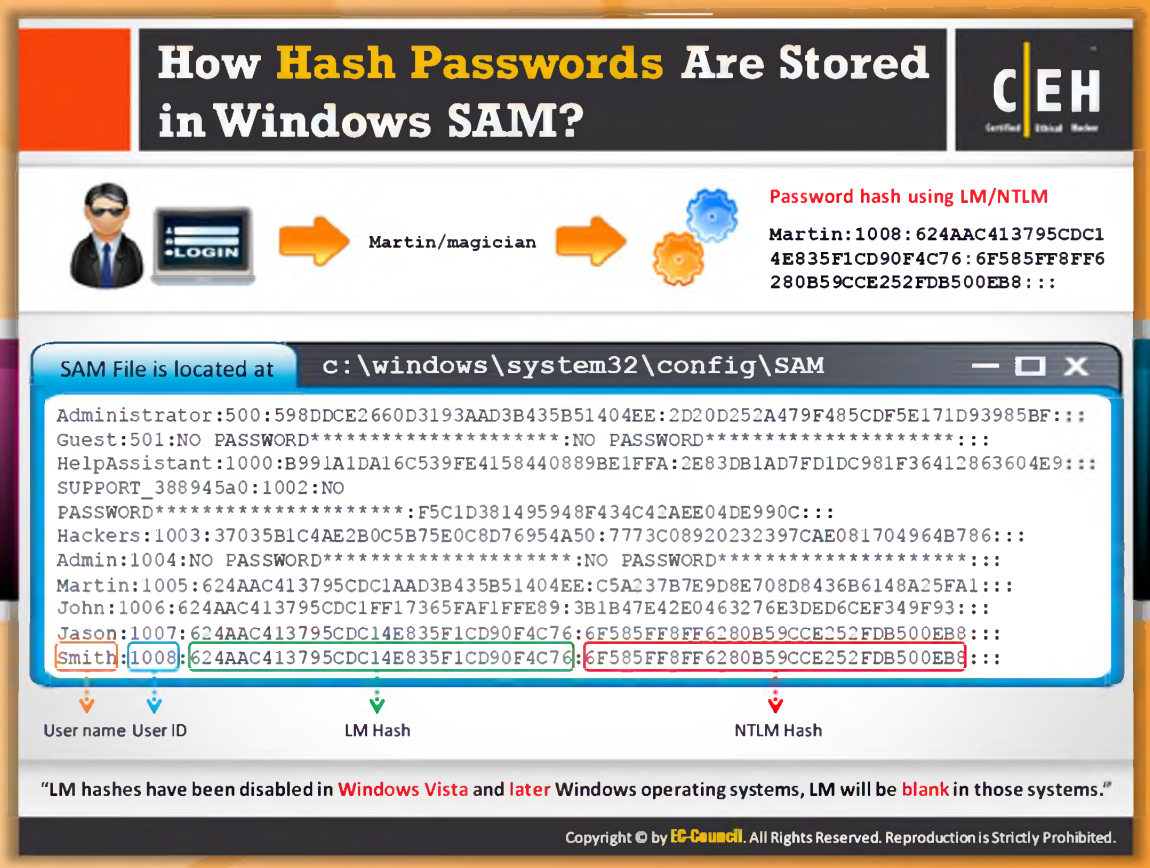
The lack of the availability of this authentication scheme in the Java platform could spell serious trouble in the development and deployment of cooperative applications based on technologies such as SOAP Web Services that rely on HTTP protocol.

Kerberos

Kerberos is a network **authentication protocol**. It is designed to provide strong authentication for client/server applications by using **secret-key cryptography**. This provides mutual authentication. Both the server and the user verify the identity of each other. Messages sent through Kerberos protocol are protected against replay attacks and eavesdropping.

Kerberos makes use of **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 works on the basis of "**tickets**" to prove the user's identity.

FIGURE 5.13: Security Authentication in Window



How Hash Passwords Are Stored in Window SAM

The **Windows XP passwords** are stored in the SAM file in a hashed format. Passwords are hashed using the LM/NTLM hash.

Martin:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8::
:

The hashes are stored in c:\windows\system32\config\SAM.

Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E171D93
985BF:::

Guest:501:NO PASSWORD*********************:NOPASSWORD*********************:::

HelpAssistant:1000:B991A1DA16C539FE4158440889BE1FFA:2E83DB1AD7FD1DC981F36412863
604E9:::

SUPPORT_388945a0:1002:NO
PASSWORD*********************:F5C1D381495948F434C42A

EE04DE990C:::

Attackers:1003:37035B1C4AE2B0C5B75E0C8D76954A50:7773C08920232397CAE081704964B7
86:::

Admin:1004:NOPASSWORD**********:NOPASSWORD**********:
::

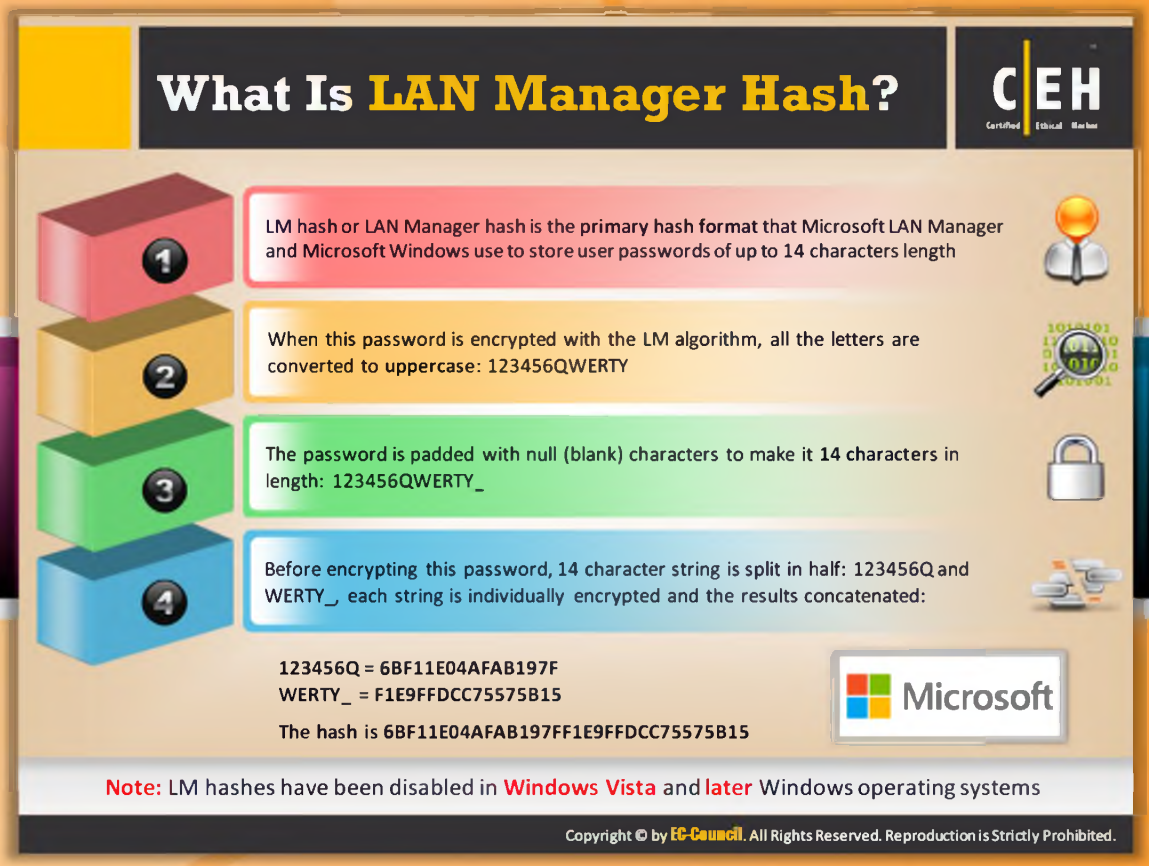
Martin:1005:624AAC413795CDC1AAD3B435B51404EE:C5A237B7E9D8E708D8436B6148A25FA
1:::

John:1006:624AAC413795CDC1FF17365FAF1FFE89:3B1B47E42E0463276E3DED6CEF349F93:::

Jason:1007:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::

Smith:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::

When the user changes his or her password, the creation and storage of valid **LM hashes** is disabled in many versions of Windows. This is the default setting for Windows Vista and Windows 7. The LM hash can be blank in the versions in which disabled LM hash is the default setting. 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. **Activating** the option additional check stores a "dummy" value in the SAM database and has no relationship to the user's password and is same for all user accounts. LM hashes cannot be calculated for the 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.



What Is a LAN Manager Hash?

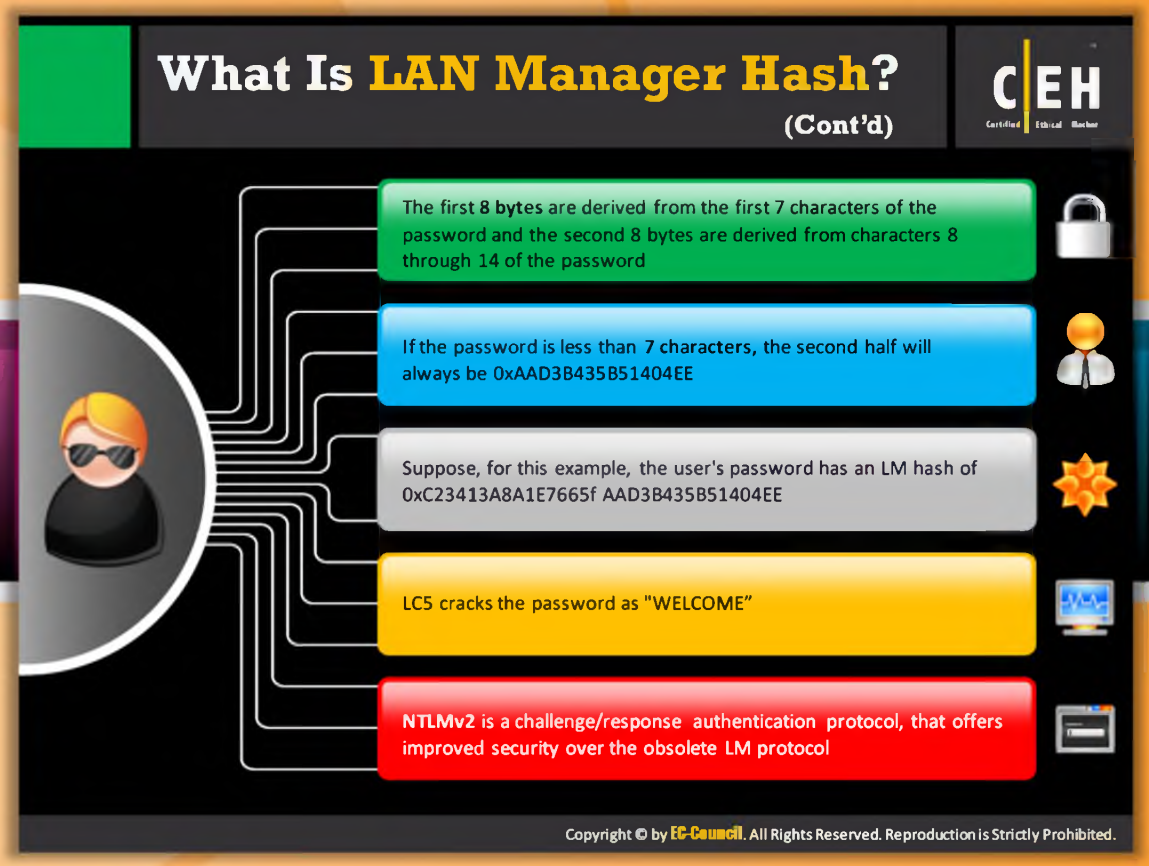
The LAN manager hash is the primary hash that Microsoft LAN Manager and Microsoft Windows use to store user passwords of up to **14 characters length**. This is used in the Microsoft Windows versions prior to Windows NT. It is continued in later version of Windows for backward compatibility, but was recommended by Microsoft to be turned off by administrators.

Microsoft Windows NT stores two types of passwords: a LAN Manager (LM) password and a Windows NT password. For example, let's assume your password is '123456qwerty'. When this password is encrypted with the LM algorithm, it is first converted to all uppercase: '123456QWERTY'. If the password is not of 14 characters in length, then it is padded with null (blank) characters to make it 14 characters in length. At this stage the assumed password becomes '123456QWERTY_'. Before **encrypting**, the 14 characters of the passwords are split into two seven byte halves. That means one seven byte string with '**123456Q**' and the second seven byte string with 'WERTY_'. Each string is encrypted individually and the results concatenated.

i.e., `123456Q = 6BF11E04AFAB197F`

`WERTY_ = F1E9FFDCC75575B15`

The resulting hash is `6BF11E04AFAB197FF1E9FFDCC75575B15`

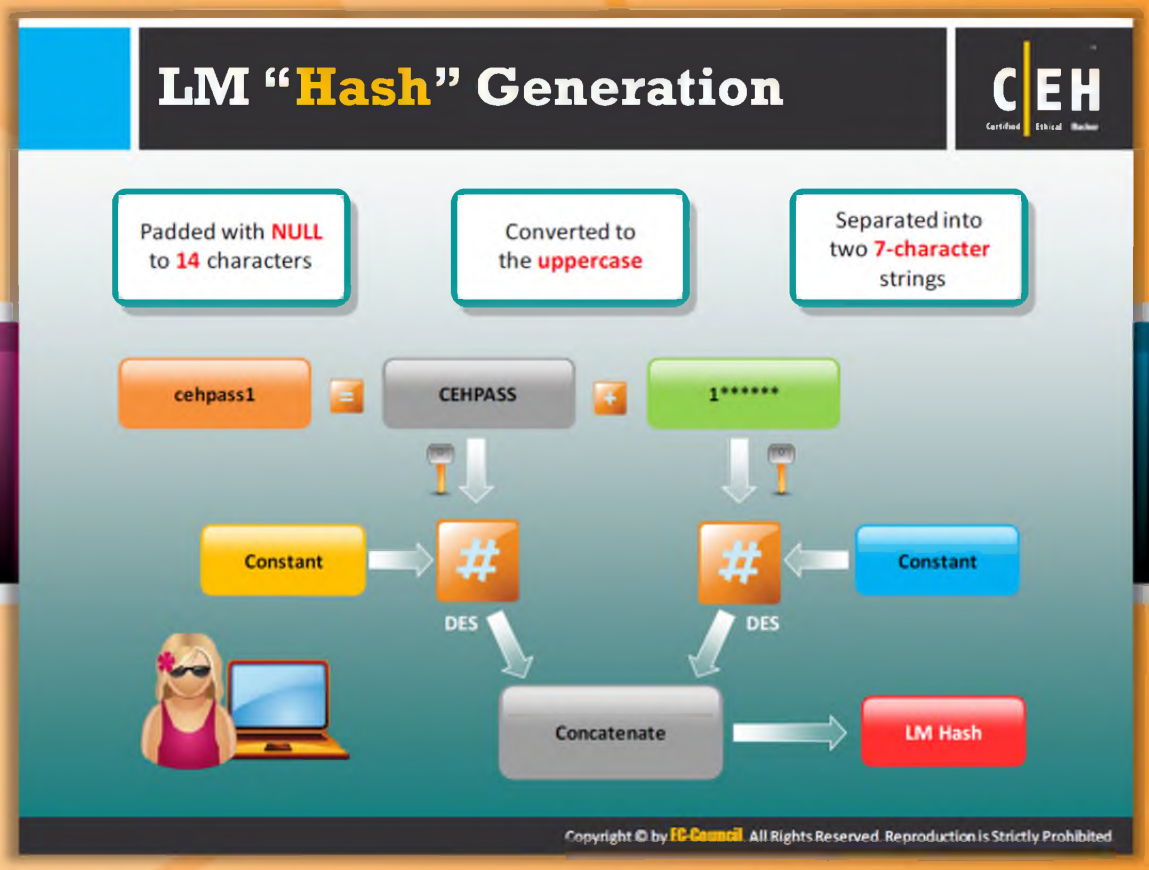


What Is LAN Manager Hash? (Cont'd)

From each **seven byte half**, an eight byte odd parity DES key is constructed. Each eight byte DES key is encrypted with a "magic number." The results of the magic number **encryption** are **concatenated** into a **sixteen byte** one-way hash value. This value is the **LAN Manager** one-way hash of the password. The first 8 bytes are derived from the first 7 characters of the password and the second 8 bytes are derived from characters 8 through 14 of the password. Together a sixteen byte one-way hash value is constructed for a password not exceeding 14 characters length.

If the password is less than or just about **7 characters in length**, then the second half is always a 0xAAD3B435B51404EE. When the **LM** password is used, it is easy for password attackers to detect the eighth character, if it is present. For example, if the user password has an LM hash of 0xC23413A8A1E7665f AAD3B435B51404EE, LC5 cracks the password as 'WELCOME' with very little effort.

NTLMv2 is a challenge/response authentication protocol that offers improved security over the obsolete LM protocol. Therefore, these systems have to set the **LAN Manager Authentication** Level to "Send NTLMv2 responses only."



LM "Hash" Generation

The LM hash also called as the LAN manager hash used by many versions of Windows for storing passwords less than 15 characters.

The following figure explains the process of generating an LM hash for a user password "cehpass1".

In the LM hash generation process, first the password in lowercase is converted to uppercase; in this example, this operation results in "CEHPASS1". Then, the uppercase password, i.e., "CEHPASS1", is divided into two seven character strings; in the example, the resulting strings are "CEHPASS" and "1******". As the second string contains only one character, to make the second string a **seven-character** string, it is lengthened with null (blank) characters, i.e., padding. The two seven-character strings are then used as the encryption keys for the encryption of a constant using the DES (Digital Encryption Standard) **symmetric cipher**. At last, to create the LM hash, the resulting **DES-encrypted blocks** are concatenated.

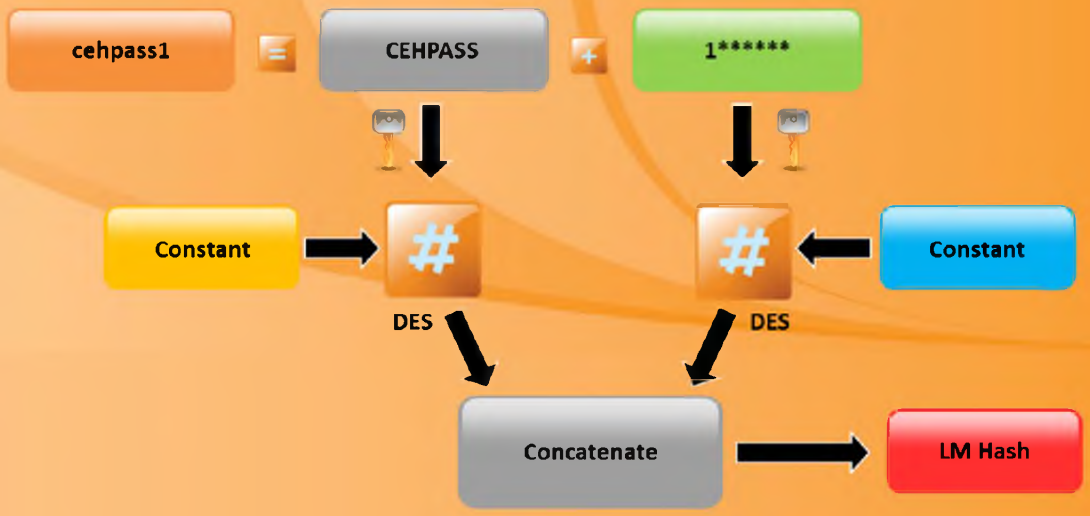
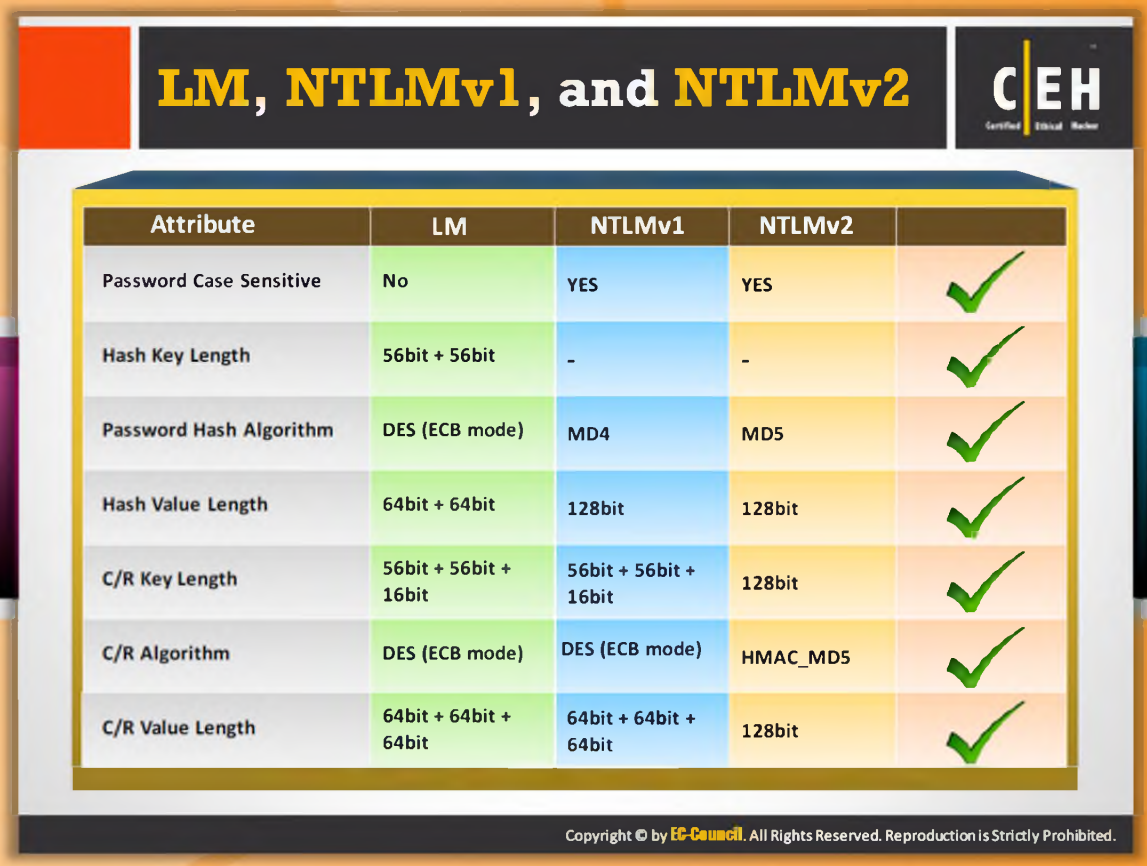


FIGURE 5.14: LM "Hash" Generator

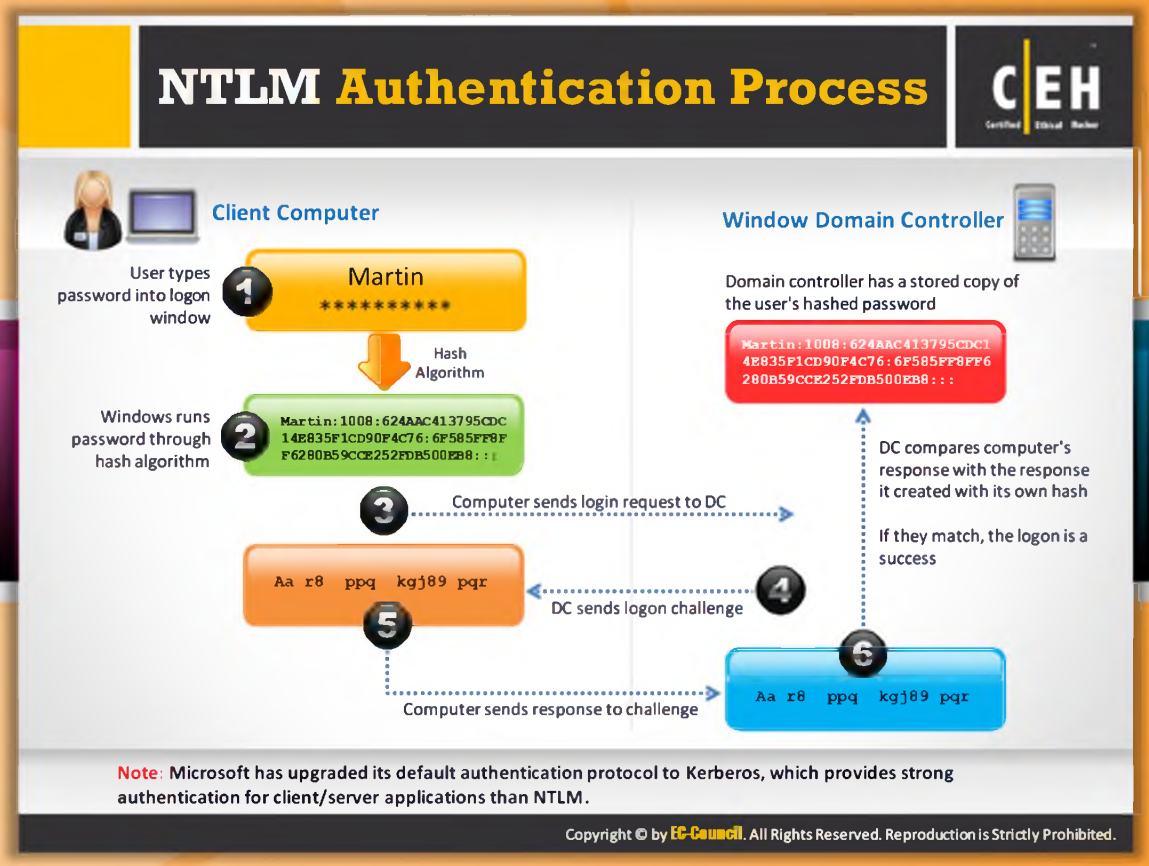


LM, NTLMv1, and NTLMv2

To address the problems in NTLM1, Microsoft introduced NTLM version 2, and advocated its use wherever possible. The following table lists the features of the three authentication methods.

Attribute	LM	NTLMv1	NTLMv2
Password Case Sensitive	No	YES	YES
Hash Key Length	56bit + 56bit	-	-
Password Hash Algorithm	DES (ECB mode)	MD4	MDS
Hash Value Length	64bit + 64bit	128bit	128 bit
C/R Key Length	56bit + 56bit +16bit	56bit + 56bit +16bit	128 bit
C/R Algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MDS
C/R Value Length	64bit + 64bit +64bit	64bit + 64bit +64bit	128 bit

TABLE 5.2: LM, NTLMv1, and NTLMv2



NTLM Authentication Process

NTLM includes three methods of **challenge-response** authentication: LM, NTLMv1, and NTLMv2. The authentication process for all the methods is the same. 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 process and the flow of the client authentication to a **domain controller** using any of the NTLM protocols is demonstrated in the following steps:

- The client types the user name and password in to 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. If the values match, the client is **authenticated** and the logon is success.

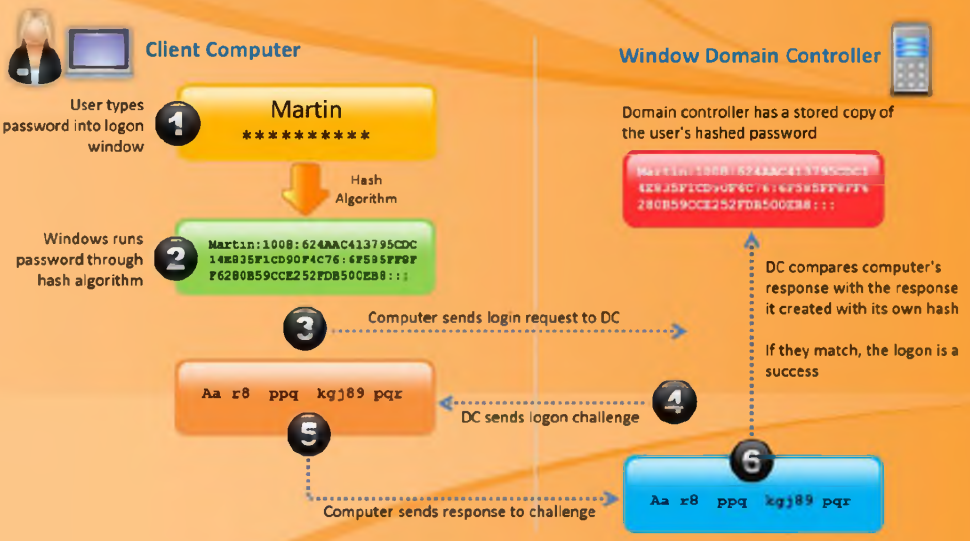
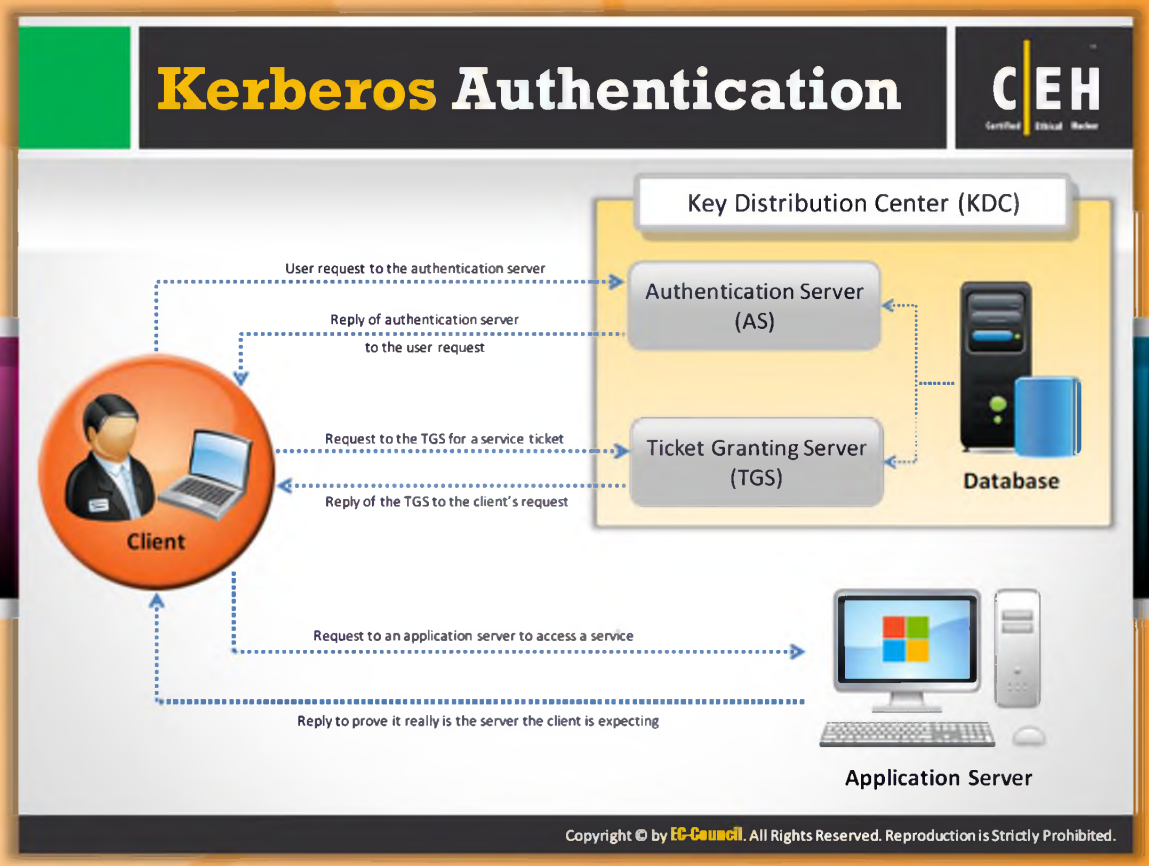


FIGURE 5.15: NTLM Authentication Process



Kerberos Authentication

Kerberos is a network authentication protocol. It is designed to provide strong authentication for **client/server applications** by using **secret-key cryptography**. This provides mutual authentication. Both the server and the user verify the identity of each other. Messages sent through **Kerberos protocol** are protected against replay attacks and **eavesdropping**.

Kerberos makes use of **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).

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 is not required to re-enter the password again for accessing any services that he is authorized for. It is important to note that there will be no direct communication between the application servers and Key Distribution Center (KDC); the service tickets, even if packeted by **TGS**, reach the service only through the client wishing to access them.

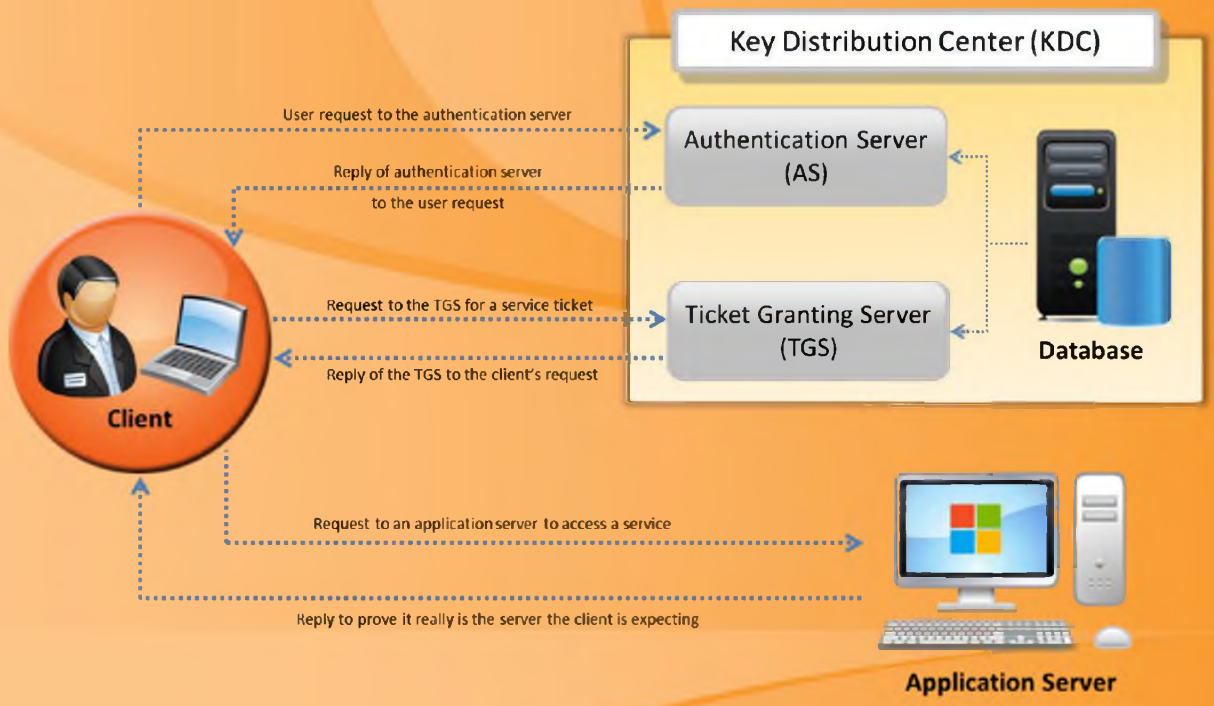
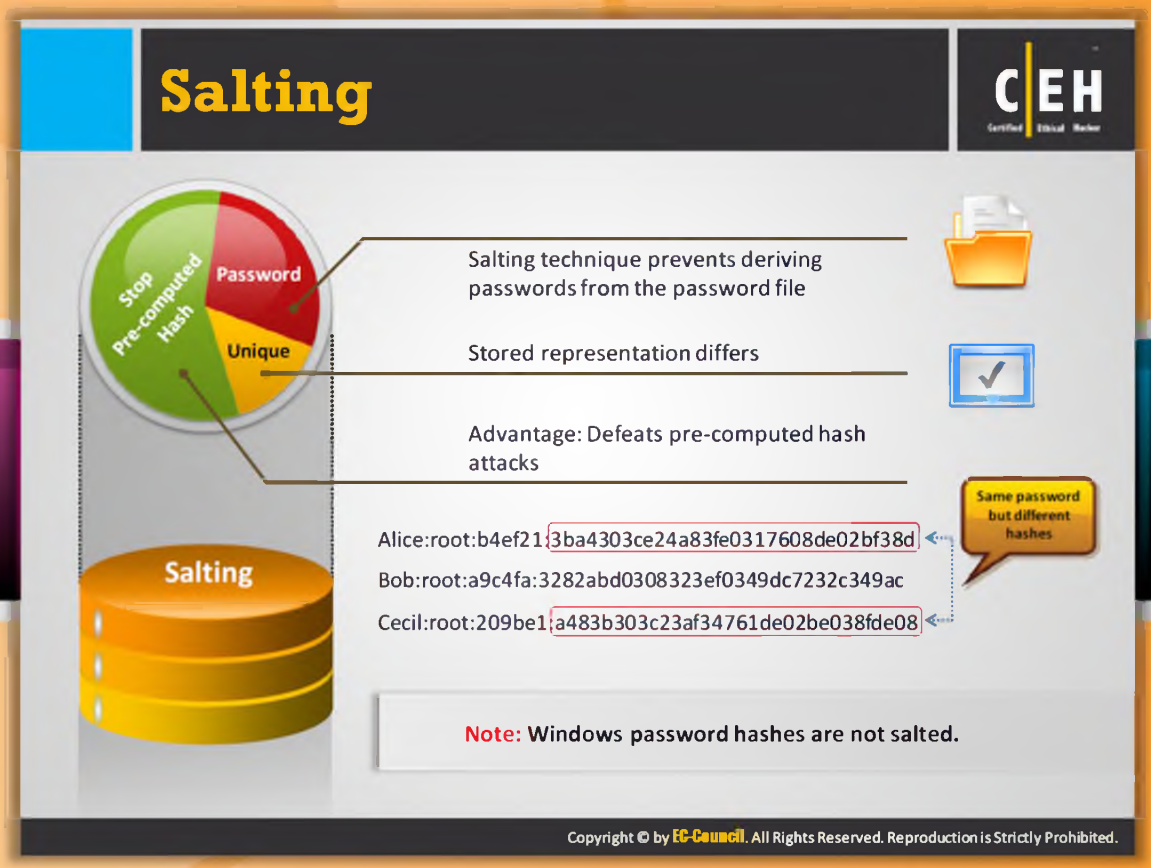


FIGURE 5.16: Kerberos Authentication



Salting

Salting is a way of making passwords more secure by adding random strings of characters to passwords before their **md5 hash** is calculated. This makes cracking passwords harder. 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**. The security level or the strength of protection of your passwords against various password attacks depends on the length of the **random string** of characters. This defeats pre-computed hash attacks.

In cryptography, a salt consists of random bits that are used as one of the inputs to a one-way function and the other input is a password. **Instead of passwords**, the output of the one-way function can be stored and used to authenticate users. A salt can also be combined with a password by a key derivation function to generate a key for use with a cipher or other **cryptographic algorithm**.

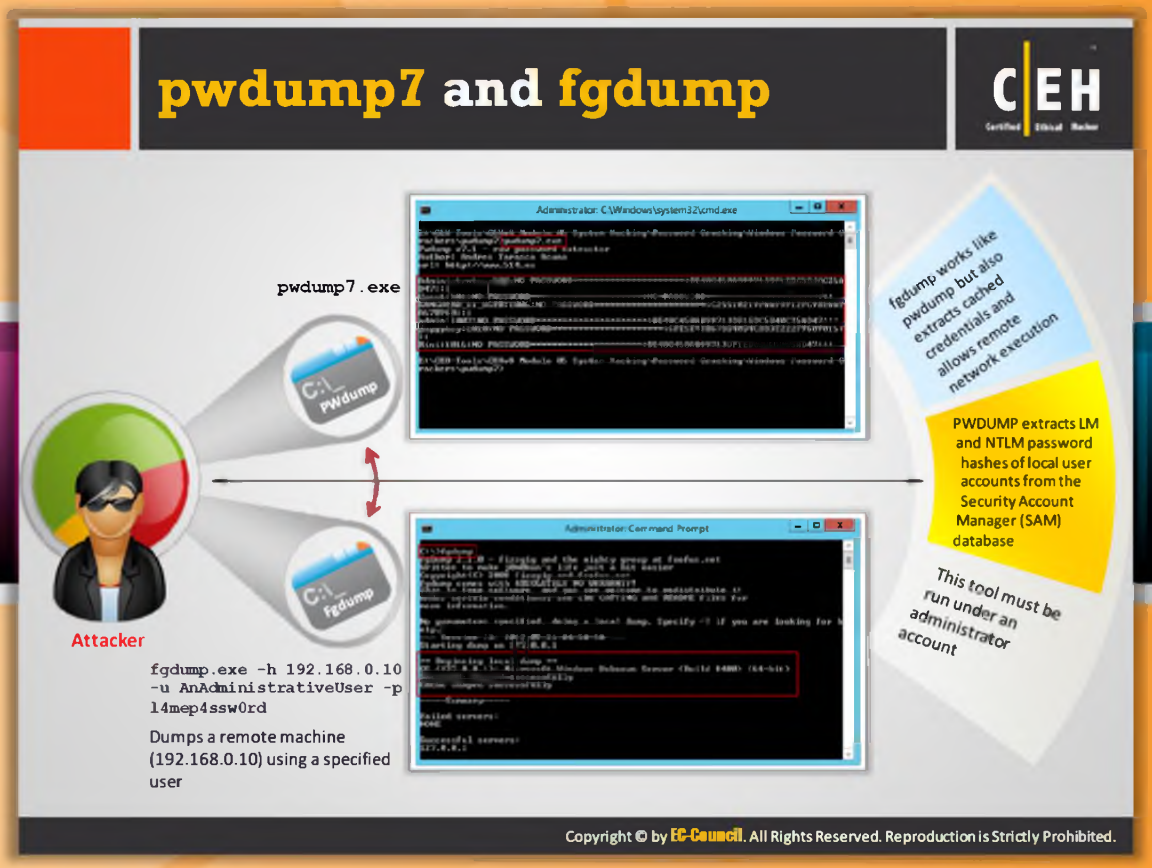
With this technique different hashes can be generated for the same password. This makes the **attacker's job of cracking** the passwords difficult.

In this example, the two users Alice and Cecil have the same passwords but with different hash values. Since a random hash is generated for each individual user:

Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d

Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac

Cecil:root:209be1:a483b303c23af34761de02be038fde08



pwdump7 and fgdump

pwdump7 is an application that dumps the password hashes (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 filesystem and then the hashes are extracted. One of the powerful features of pwdump7 is that it is also capable of **dumping** protected files. Usage of this program requires **administrative privileges** on the remote system.

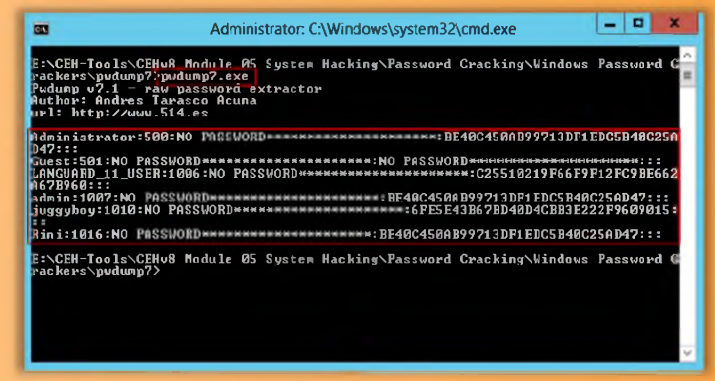


FIGURE 5.18: pwdump7 Extracting Raw Password in Window

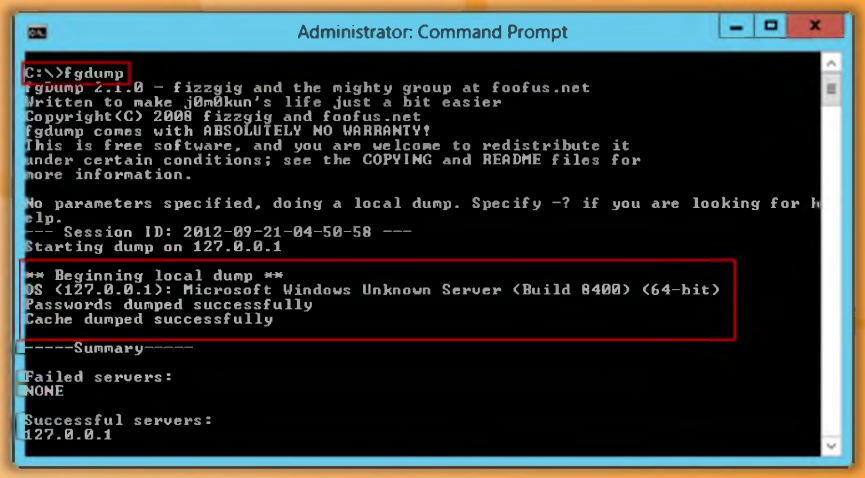
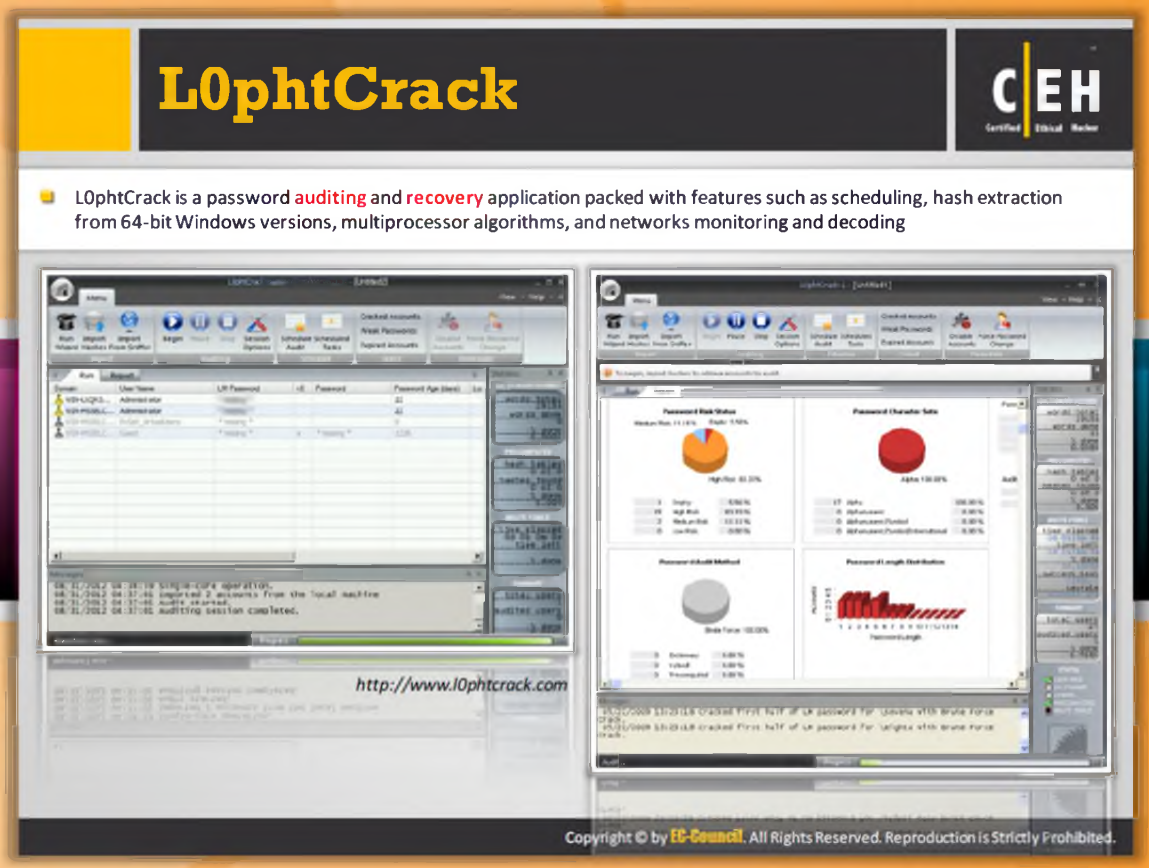


FIGURE 5.19: fgdump Dumping Password in Window

fgdump is basically 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 also do a number of other **crucial things** like executing a remote executable and dumping the **protected storage** on a remote or local host, and **grabbing cached credentials.**



L0phtCrack

Source: http://www.l0phtcrack.com

L0phtCrack is a tool designed to audit password and recover applications. It is used to recover lost Microsoft Windows passwords with the help of dictionary, hybrid, rainbow table, and brute force attacks and it is also used to check the strength of the password. The security defects that are **inherent** in windows **password authentication** system can be disclosed easily with the help of LOphtCrack.

Windows operating systems, based on the **LAN Manager** networking protocols, use an authentication system that consists of an 8-byte challenge returning a 24-byte response across the network from client to server in a challenge/response format. The server matches the response against its own independent calculation of the **24-byte** response expected and the match results in **authentication**. The algorithm divides the password into **seven-character segments** and then hashes individually. This allows the attacker to restrict the password cracking to seven letters and makes the process easier. The weakness of the password hash, coupled with the transmission of the hash across the network in the challenge/response format, makes LM-based systems highly susceptible to challenge/response interception followed by dictionary and **brute-force attacks** by L0phtCrack. **L0phtCrack** 6 has the built-in ability to import passwords from remote Windows, including 64-bit versions of Vista, Windows 7, and Unix machines, without requiring a **third-party utility**.

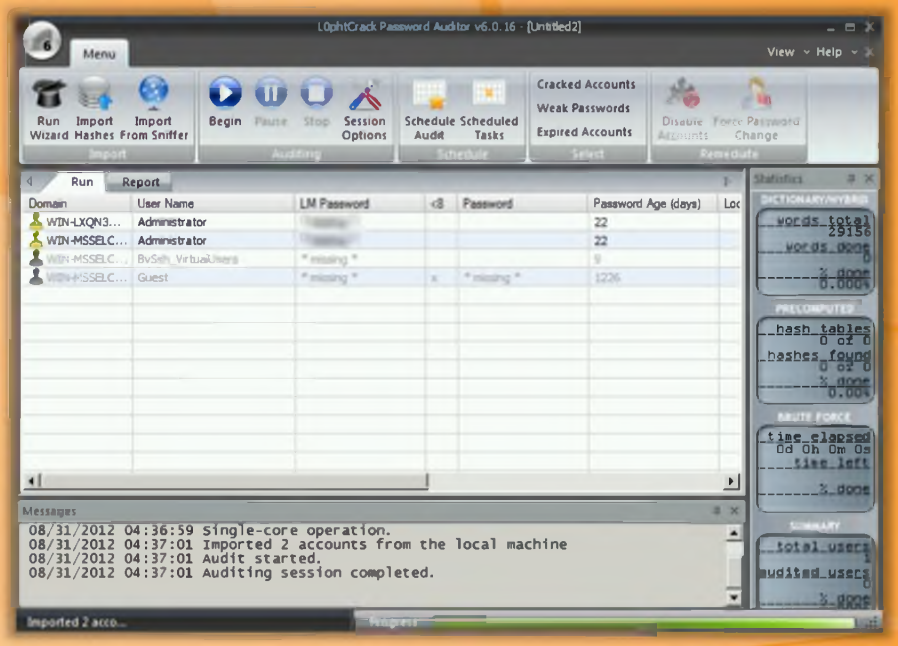


FIGURE 5.20: L0phtCrack in Run Mode

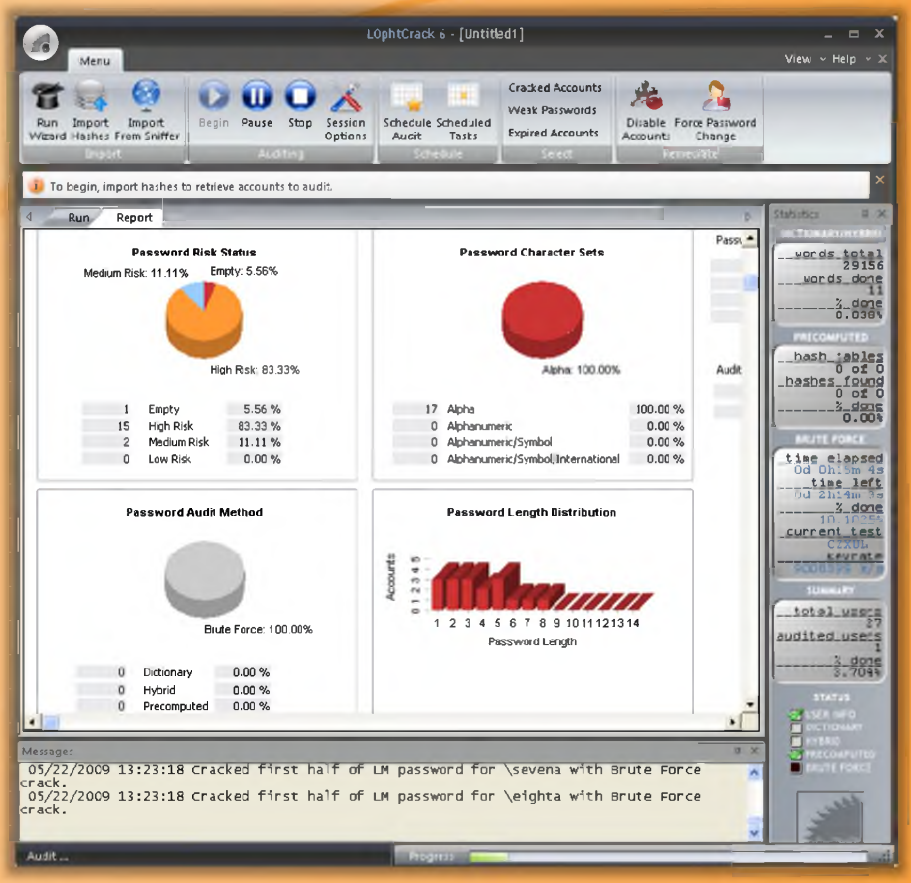
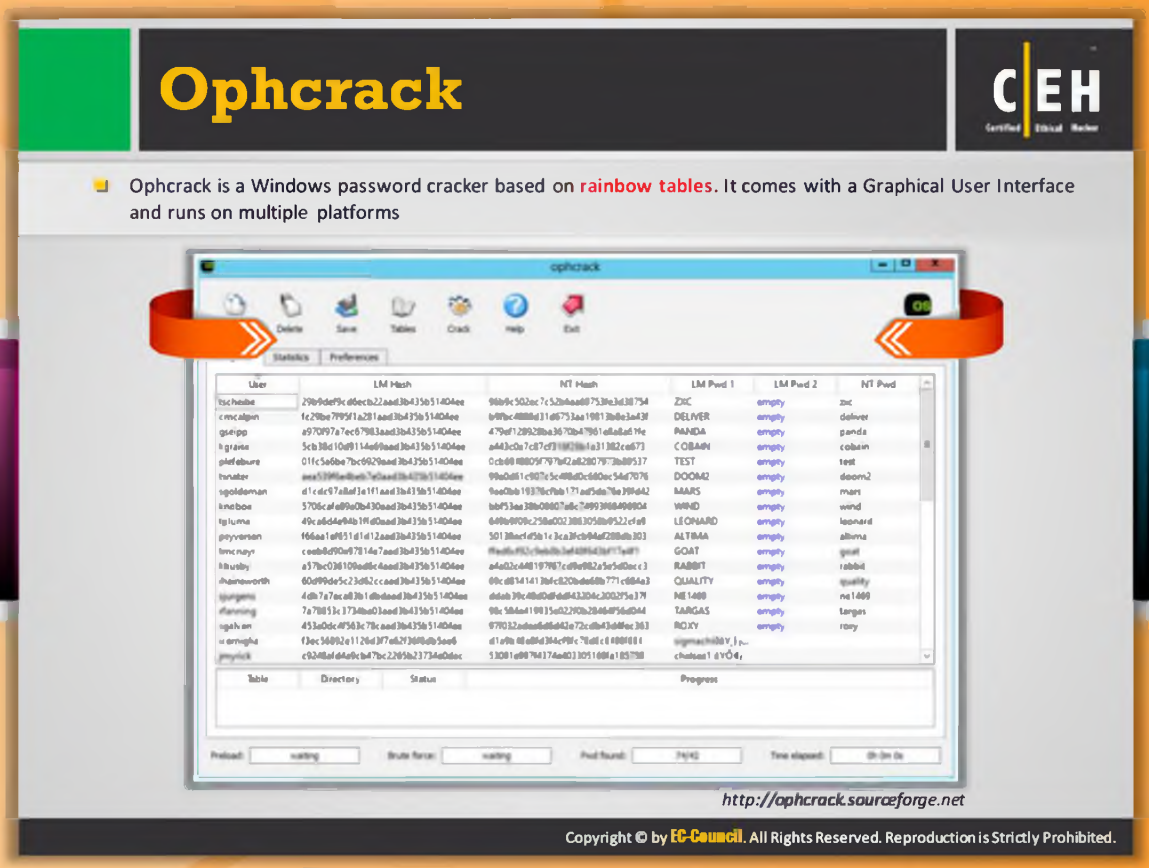


FIGURE 5.21: L0phtCrack in Report Mode



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.

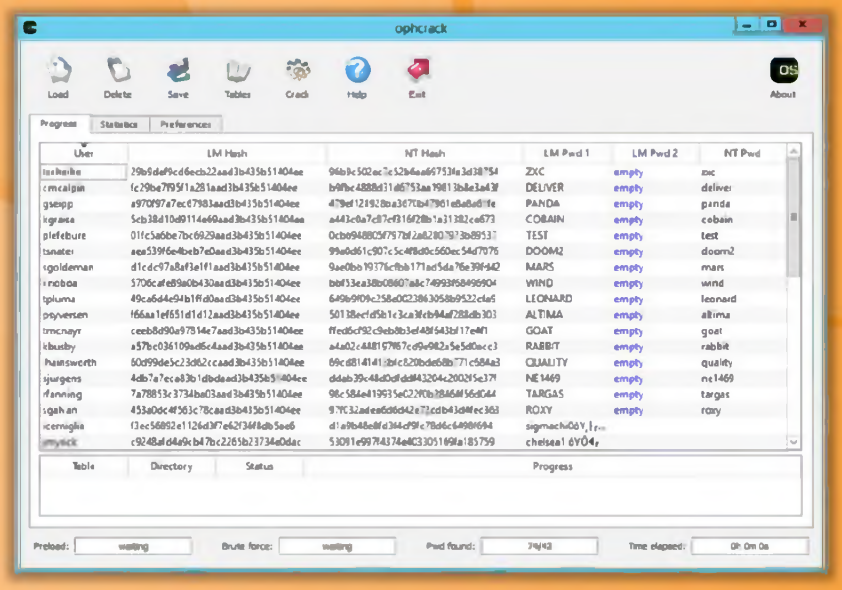
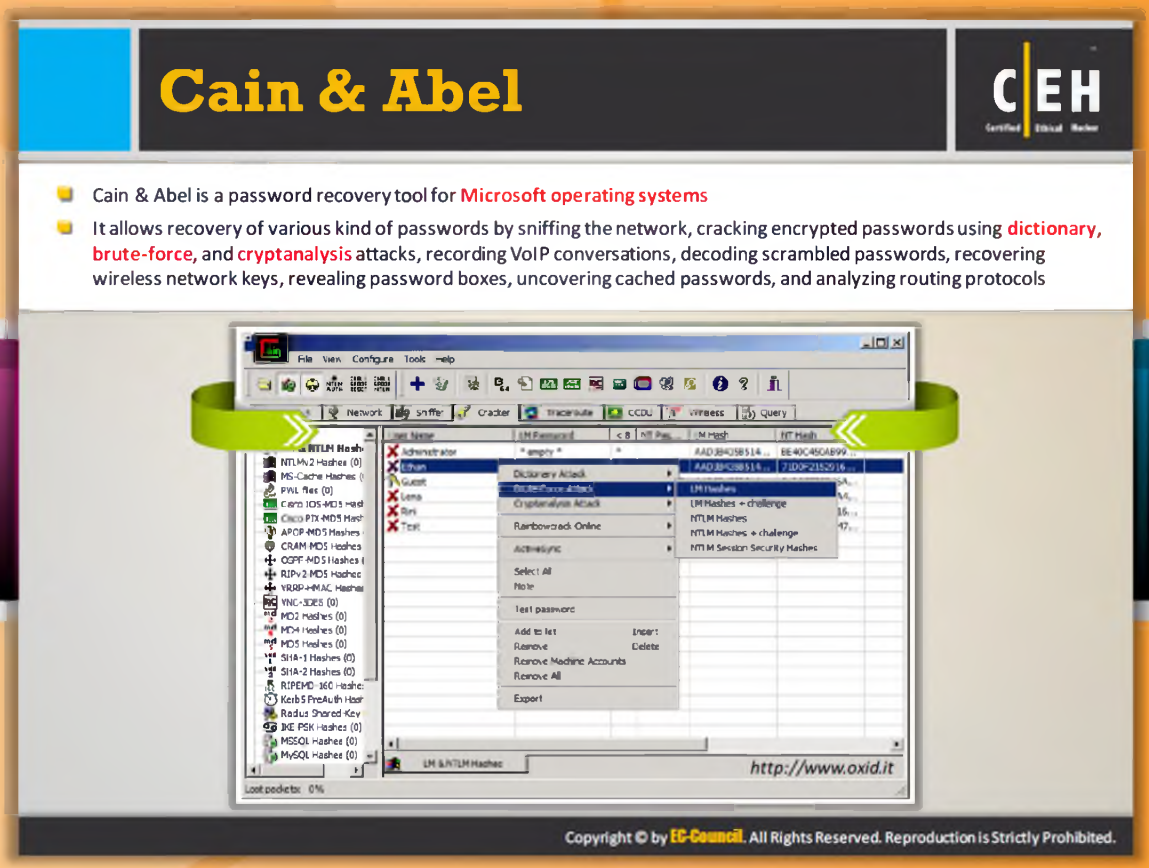


FIGURE 5.22: Ophcrack Screenshot



Cain & Abel

Source: http://www.oxid.it

Cain & Abel is a password recovery tool. It runs on the **Microsoft operating system**. It allows you to recover various kinds of passwords by **sniffing** the network, cracking encrypted passwords using 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. With the help of this tool, passwords and **credentials** from various sources can be recovered easily.

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

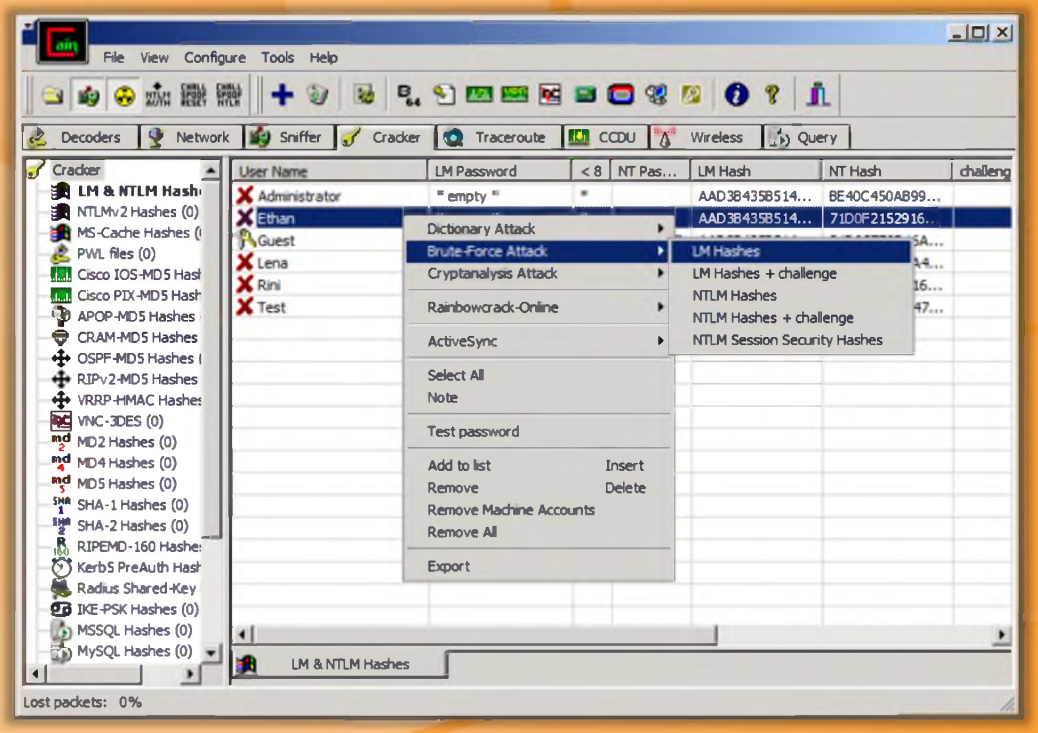
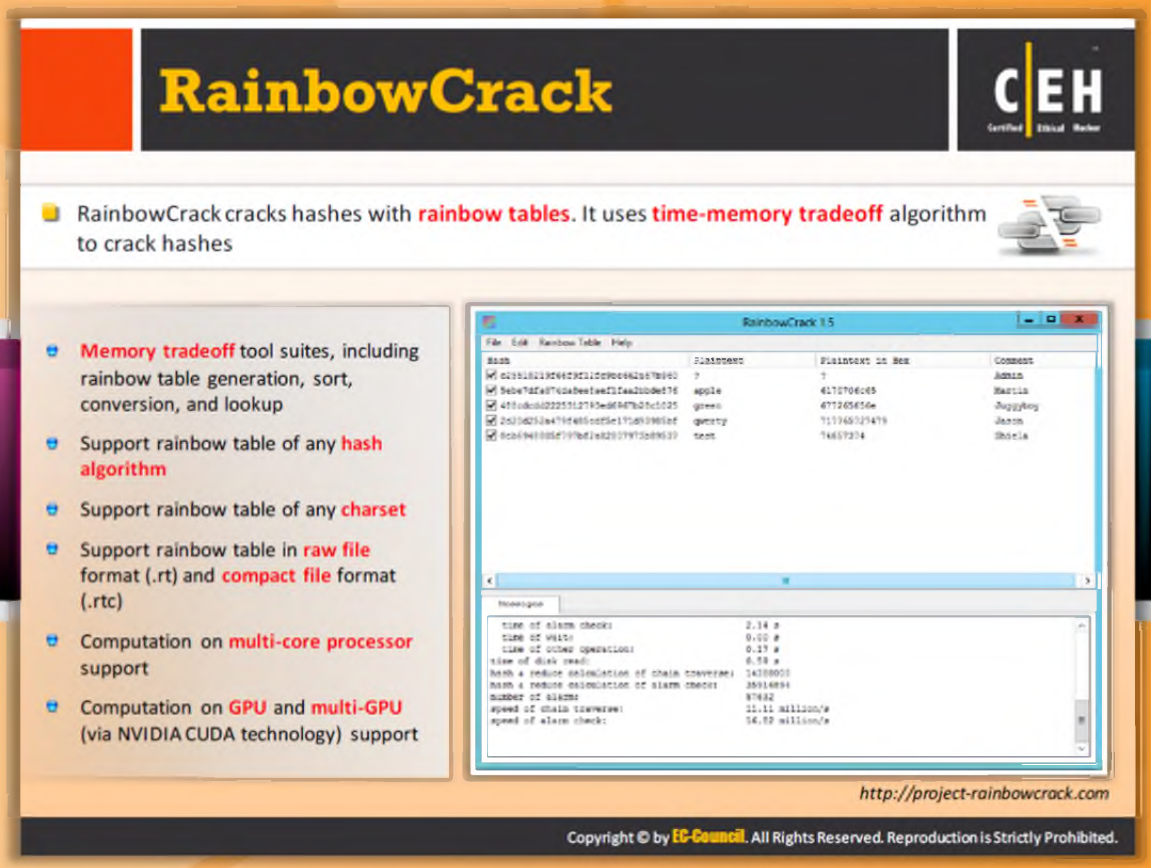


FIGURE 5.23: Cain & Abel Screenshot



RainbowCrack

Source: http://project-rainbowcrack.com

RainbowCrack cracks hashes with rainbow tables. It uses a time-memory tradeoff algorithm to crack hashes. A traditional **brute force cracker** cracks hashes differently when compared to 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-**ciphertext pairs** 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**.

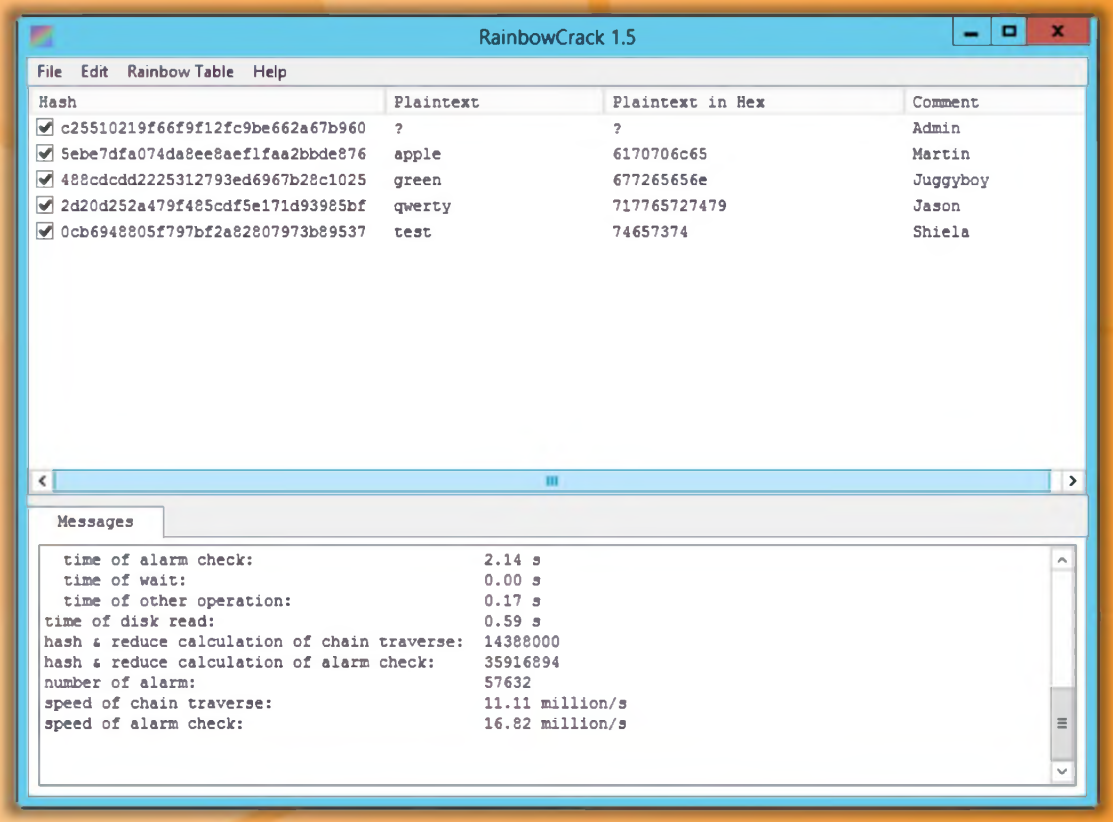
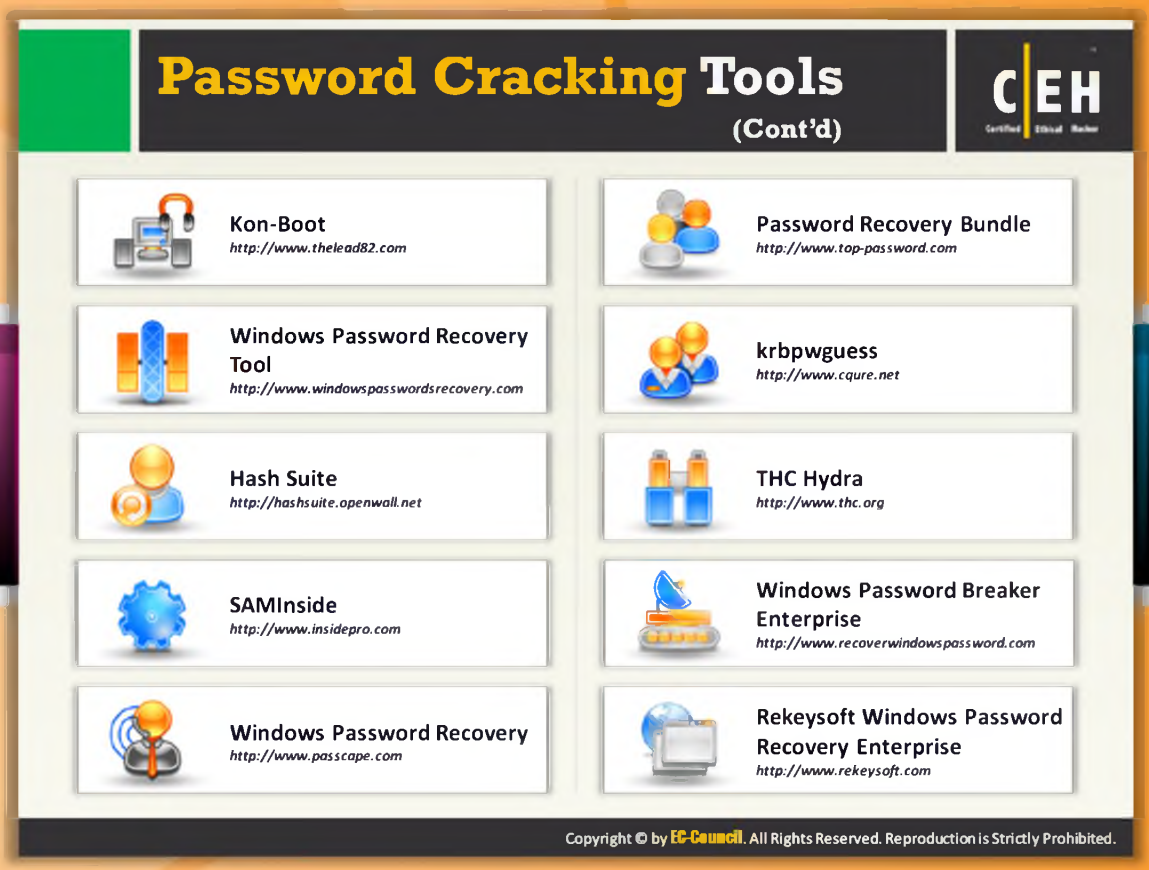


FIGURE 5.24: RainbowCrack Screenshot

Password Cracking Tools

Password cracking tools allow you to reset unknown or lost **Windows local administrator**, domain administrator, and other user account passwords. It even allows users to get access to their locked computer instantly without **reinstalling** Windows, in case of forgotten passwords. A few passwords **cracking tools** are listed as follows:

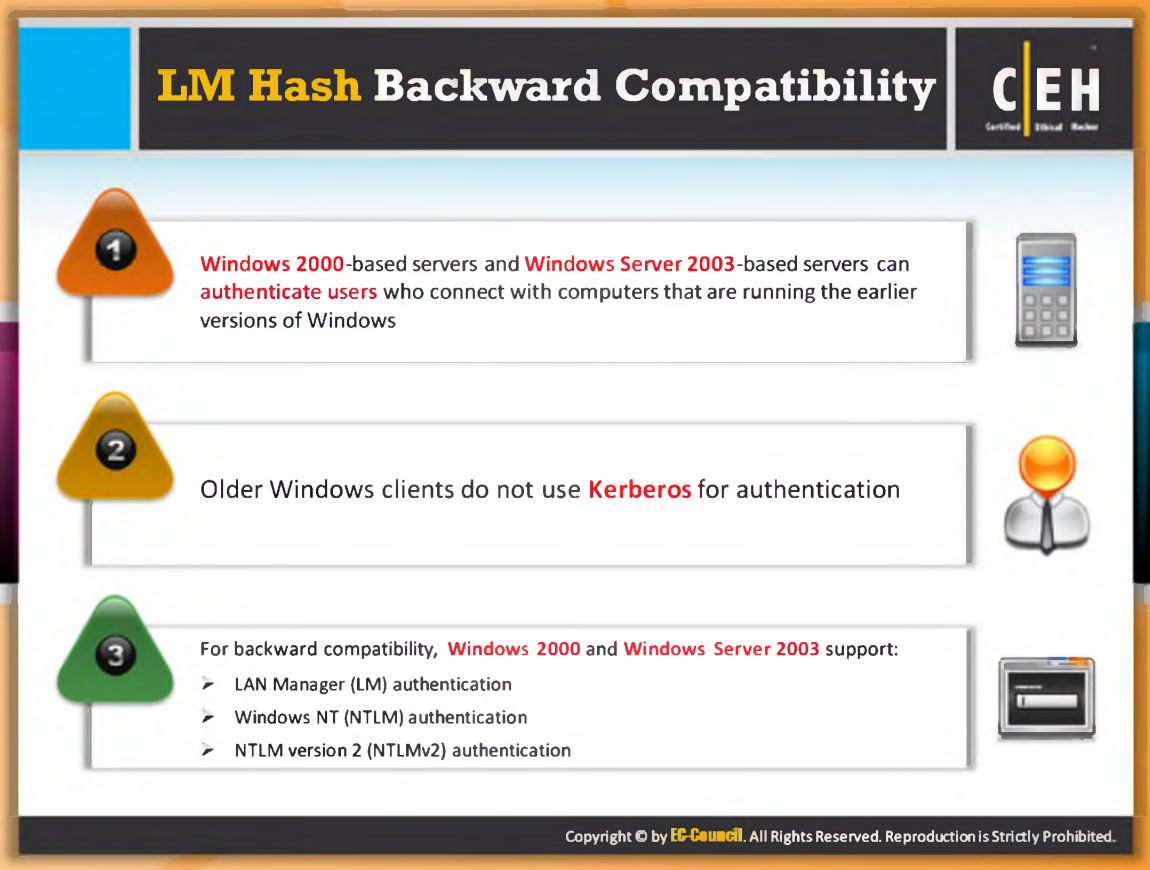
- Password Unlocker Bundle available at http://www.passwordunlocker.com
- Proactive System Password Recovery available at http://www.elcomsoft.com
- John the Ripper available at http://www.openwall.com
- Windows Password Cracker available at http://www.windows-password-cracker.com
- WinPassword available at http://lastbit.com
- Passware Kit Enterprise available at http://www.lostpassword.com
- PasswordsPro available at http://www.insidepro.com
- LSASecretsView available at http://www.nirsoft.net
- LCP available at http://www.lcpsoft.com
- Password Cracker available at http://www.amlpages.com



Password Cracking Tools (Cont'd)

The list of password cracking tools continues as follows:

- **Kon-Boot** available at http://www.thelead82.com
- Windows Password Recovery Tool available at http://www.windowspasswordsrecovery.com
- Hash Suite available at http://hashsuite.openwall.net
- SAMInside available at http://www.insidepro.com
- **Windows Password Recovery** available at http://www.passcape.com
- Password Recovery Bundle available at http://www.top-password.com
- Krbpwguess available at http://www.cqure.net
- THC Hydra available at http://www.thc.org
- Windows Password Breaker Enterprise available at http://www.recoverwindowspassword.com
- Rekeysoft Windows Password Recovery Enterprise available at http://www.rekeysoft.com



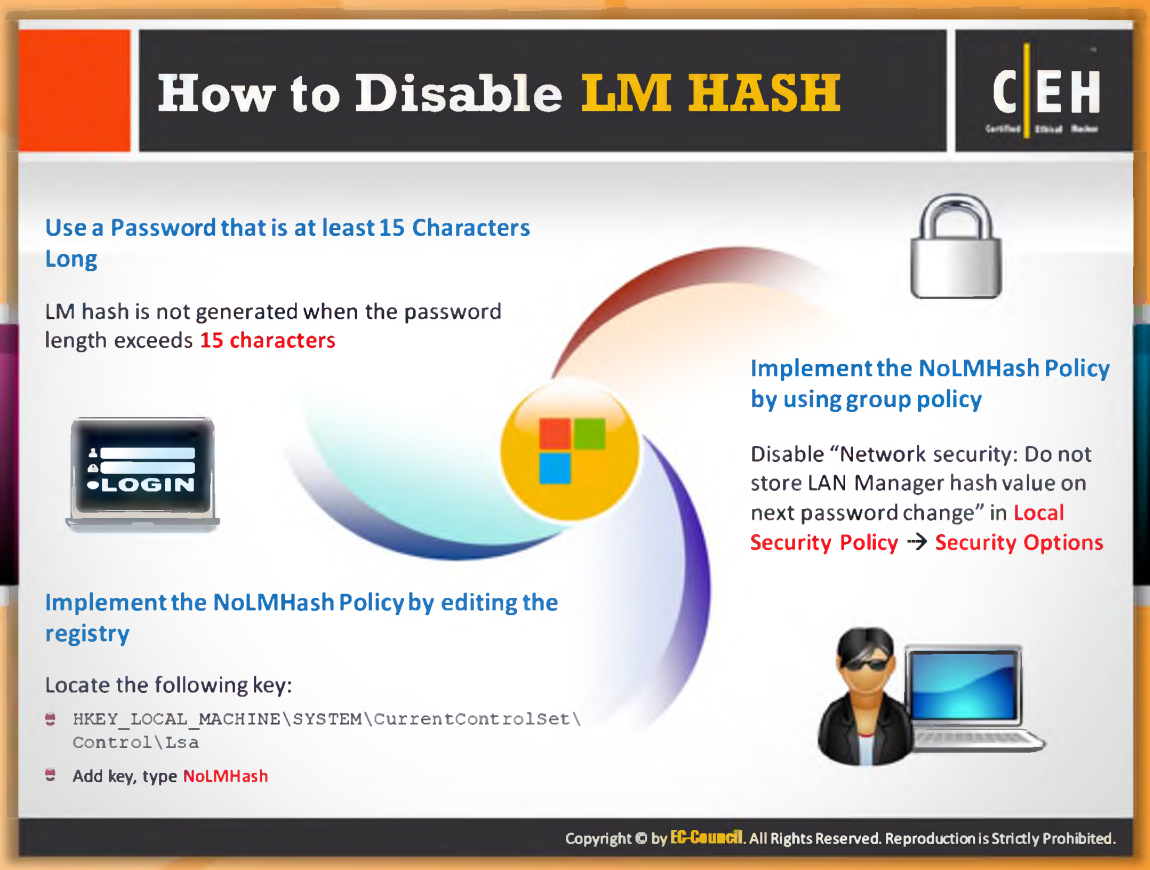
LM Hash Backward Compatibility

LM Hash Backward Compatibility is a server based on Windows 2000 and Windows server 2003 and can **authenticate** users that are running all versions of Windows. Windows 95/98 clients do not use **Kerberos** for authentication.

For backward compatibility, Windows 2000 and **Windows Server 2003** support:

- LAN Manager (LM) authentication
- Windows NT (NTLM) authentication
- NTLM version 2 (NTLMv2) authentication

An NT hash (unicode hash) is used in NTLM1, NTLMv2, and Kerberos. The **LM authentication** protocol uses the "**LM hash**." Do not store the LM hash, if it is not necessary, for backward compatibility. If LM hashes are stored, Windows95, Windows98, or **Macintosh clients** of networks may experience the backward **compatibility** problem.



How to Disable LM HASH

Method 1: Implement the NoLMHash Policy by Using a Group Policy

To disable the storage of LM hash in the SAM databases by applying the local group policy, use the steps as follows:

- In **Group Policy**, select **Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options.**
- In the list of available policies, double-click **Network security: Do not store LAN Manager hash value on next password change**.
- Click **Enabled → OK**.

Method 2: Implement the NoLMHash Policy by Editing the Registry

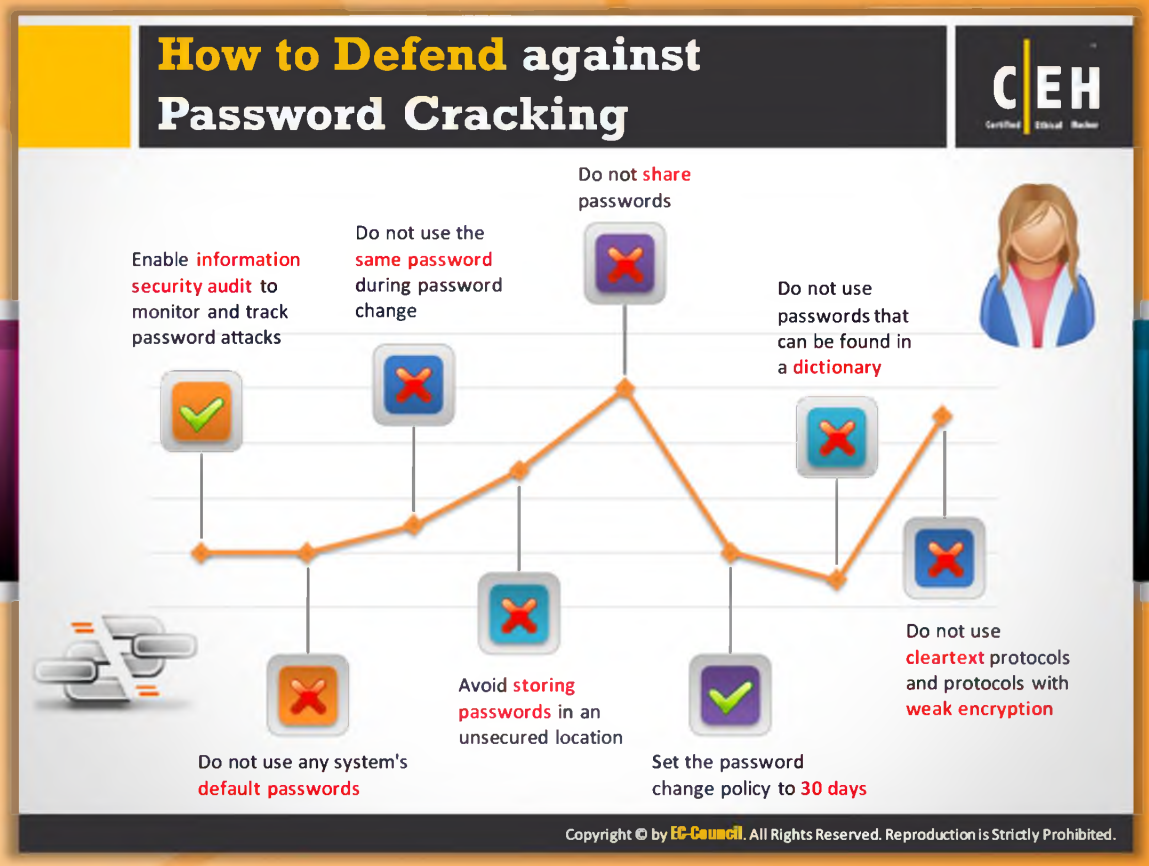
Locate the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Add the key, and type **NoLMHash**

Method 3: Use a Password that is at Least 15 Characters Long

Windows stores an LM hash value that cannot be used to authenticate the user.

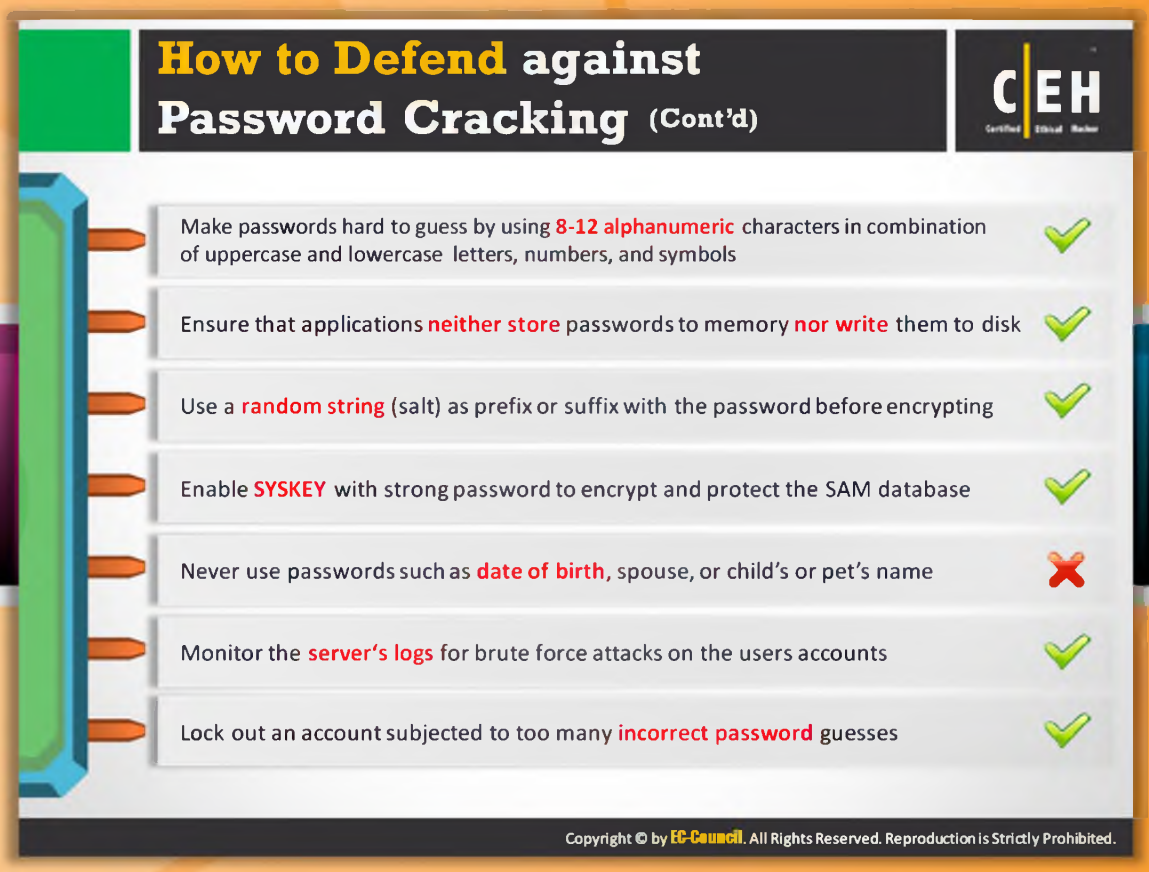


How to Defend against Password Cracking

Password cracking, also known as **password hacking**, is the term used to define the process of gaining **unauthorized** use of the network, system, or resources that are secured with a password. The basic way of password cracking is guessing the password. Another way is to try various combinations repeatedly. It is done using a **computer algorithm** where the computer tries various combinations of characters until and unless a **successful combination** occurs. If the password is weak, then it can be **cracked easily**. In order to avoid the risk of **password cracking**, there are some **best practices** that help you to defend against password cracking. They are:

- Don't share your password with anyone, as this allows another person to access your personnel information such as **grades** and pay statements, information that is normally restricted to you.
- Do not use the same password during a password change, i.e., one that is substantially similar to the previously used one.
- Enable **security auditing** to help monitor **and track password attacks**.
- Do not use passwords that can be found in a **dictionary**.
- Do not use **cleartext protocols** and protocols with weak **encryption**.

- Set the password **change policy** as often as possible, i.e., for every 30 days.
- Avoid storing passwords in an **unsecured** location because passwords that are stored in places such as in a computer files are easily subjected to attacks.
- Do not use any system's **default passwords**.



How to Defend against Password Cracking (Cont'd)

Additional best practices against password cracking include:

- Make passwords hard to guess by using eight to **twelve alphanumeric characters** in 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. If the passwords are stored to memory the passwords can be **stolen**. Once the password is known it is very easy for the attacker to escalate their rights in the application.
- Use a **random string** (salt) as prefix or suffix with the password before encrypting. This is used for nullifying pre-computation and **memorization**. Since salt is usually different for all individuals, it is impractical for the attacker to construct the tables with a single encrypted version of each candidate password. UNIX systems usually use 12-bit salt.
- 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 the **password-cracking** software to target the SAM database for accessing the passwords of user accounts. So, to avoid such instances, SYSKEY comes into the picture. **SYSKEY** provides protection to the user account password information, i.e.,

stored in the SAM data against password-cracking software using strong encryption techniques. It is more difficult to crack encrypted password information than non-**encrypted password information**.

- Never use personal information as your passwords such as date of birth, spouse, or child's or pet's name. If you use such passwords, it becomes quite easy for the people who are 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 can easily be detected by **monitoring** the web server log. For each unsuccessful login attempt, an **HTTP 401 status** code gets recorded in your web server logs.
- Lock out an account subjected to too many incorrect password guesses. This provides protection against **brute-force attacks** and **guessing**.

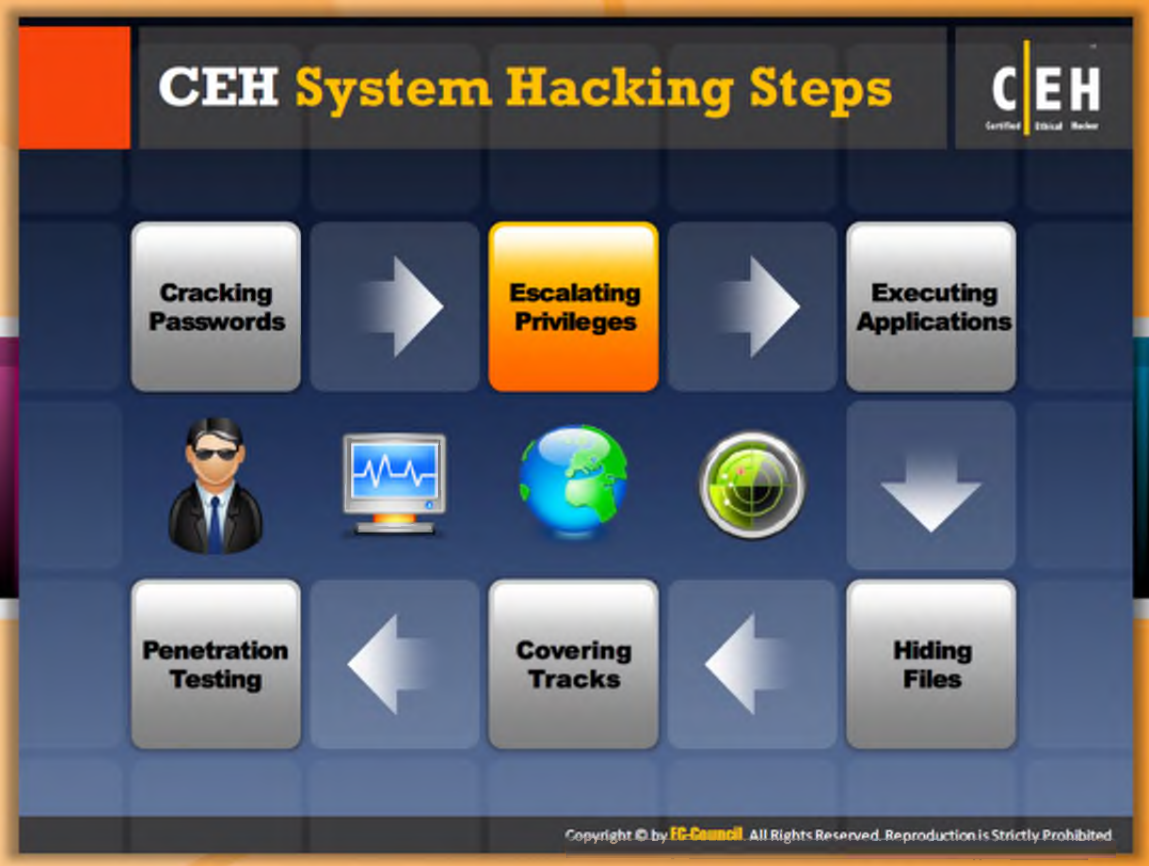
Implement and Enforce a Strong Security Policy

A **strong security policy** provides the foundations for the successful **implementation** of security-related projects in the future; this is the first measure that must be taken to reduce 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. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

The proper implementation of a strong security policy is highly beneficial as it will not only turn all of your staff into participants in the company's effort to secure its communications, but also help reduce the risk of a potential security breach through "human-factor" mistakes. These are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other dangerous activities.

Additionally, the erection process of a security policy will also help define a company's critical assets, the ways they must be protected, and will also serve as a centralized document, as far as protecting security assets is concerned.

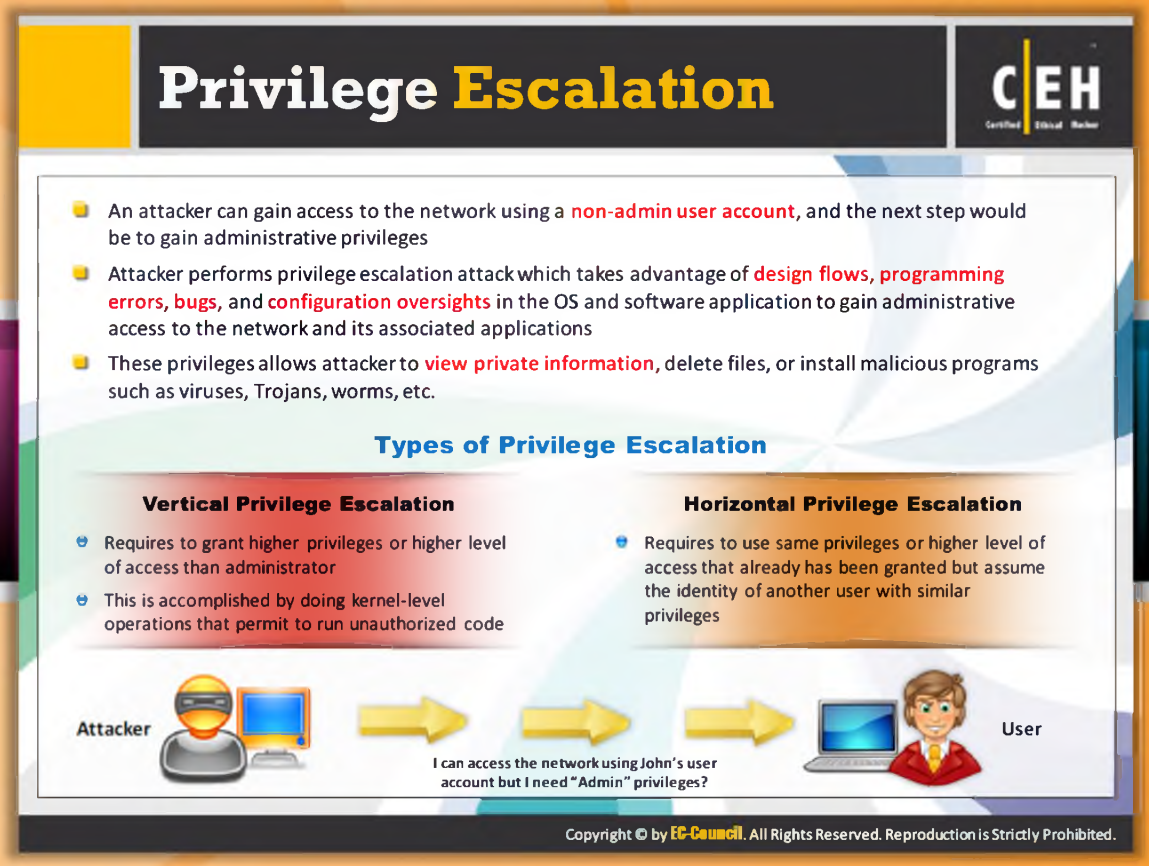
FIGURE 5.24: Implement and Enforce a Strong Security Policy



CEH System Hacking Steps

Escalating privileges is the second stage of system hacking. In this stage, an attacker uses cracked passwords to gain higher level privileges in order to carry out highly privileged operations in the target system. The various tool and techniques that are used by attackers to escalate the privileges are explained clearly in the following slides.

Cracking Passwords	Hiding Files
Escalating Privileges	Covering Tracks
Executing Applications	Penetration Testing



Privilege Escalation

In a privilege escalation attack, the attacker gains access to the networks and their associated data and applications by taking the advantage of defects in design, **software application**, poorly configured **operating systems**, etc.

Once an attacker has **gained access** to a remote system with a valid user name and password, he or she will attempt to increase his or her privileges by **escalating** the user account to one with increased privileges, such as that of an administrator. For example, if the attacker has access to a **W2K SP1 server**, he or she can run a tool such as ERunAs2X.exe to escalate his or her privileges to that of SYSTEM by using "nc.exe -l -p 50000 -d -e cmd.exe." With these privileges the attacker can easily steal personnel information, delete files, and can even deploy malicious, i.e., unwanted program such as Trojans, viruses, etc. into the victim's systems.

Privilege escalation is required when you want to gain unauthorized access to targeted systems. Basically, privilege escalation takes place in two forms. They are **vertical privilege escalation** and horizontal privilege escalation.

Horizontal Privilege Escalation: In 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 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 with administrative functions.

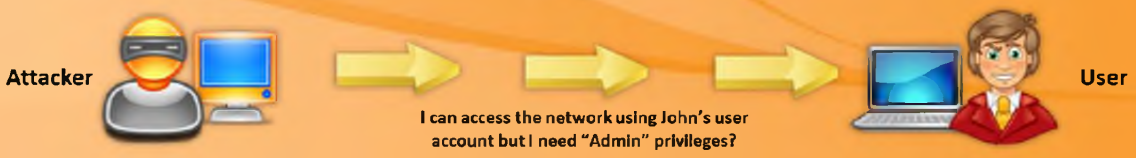
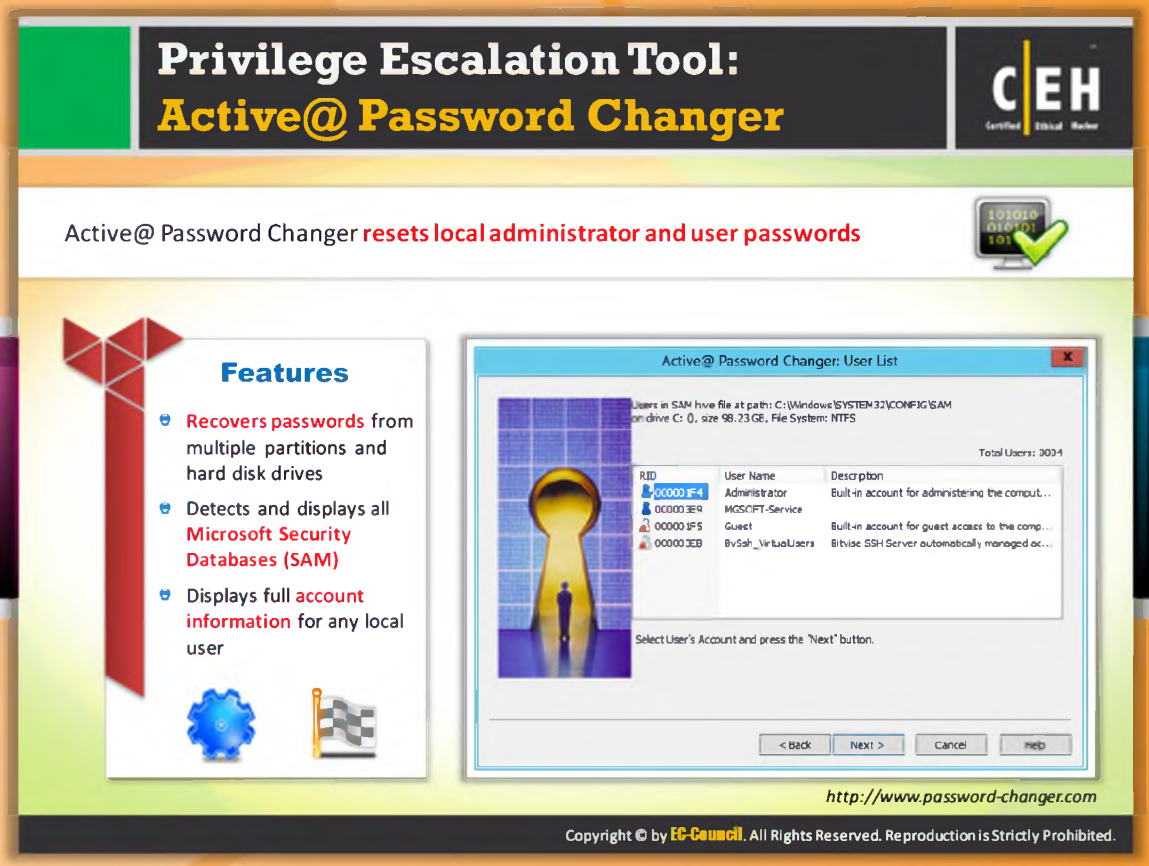


FIGURE 5.25: Working of Privilege Escalation



Privilege Escalation Tool: Active@ Password Changer

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

Active@Password Changer is a password recovery tool that **resets or recovers** the local administrator and the user passwords when the administrator has lost or forgotten his or her password or if the administrator's user account was locked out or disabled. Its main features includes **recovering passwords** from multiple partitions and hard disk drives, displaying and detecting all the Microsoft Security Databases, resetting administrator's/user's password, displaying complete account information for any local user, etc.

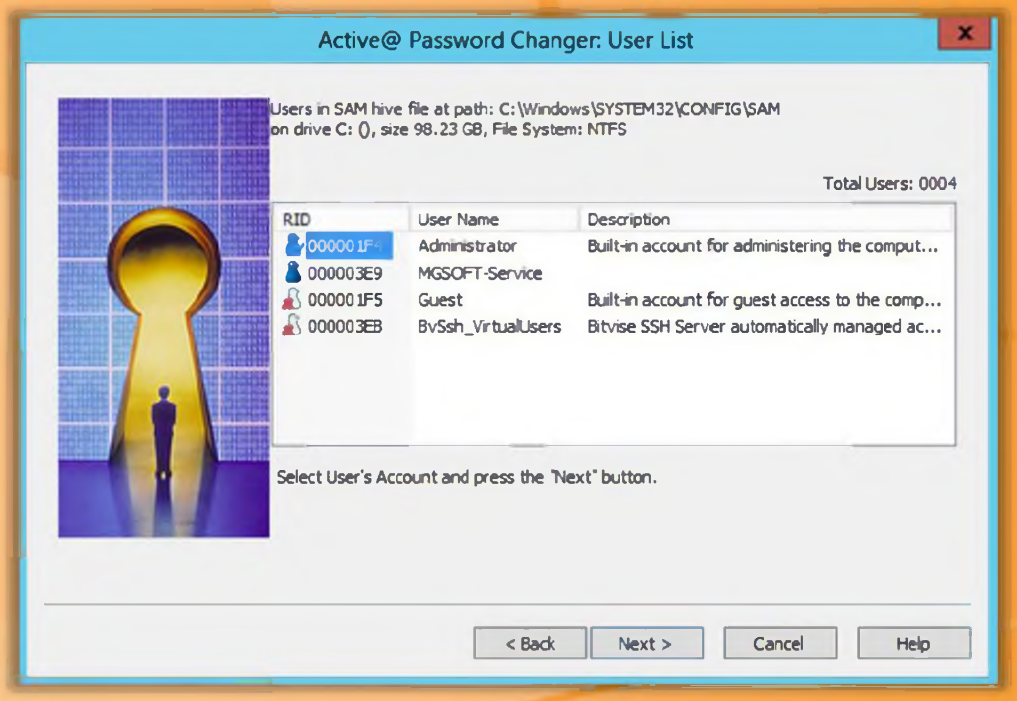


FIGURE 5.26: Active@ Password Changer Screenshot

Privilege Escalation Tools

Privilege escalation tools allow you to safely and efficiently remove, reset, or bypass Windows administrator and user account passwords in case you have lost or forgotten your password and cannot log in to your computer. With the help of these tools, you can easily gain access to the locked computer by resetting the **forgotten** or **unknown password** to blank. The attacker can use these tools for recovering the original passwords of the victim. A few privilege **escalation tools** are listed as follows:

- Offline NT Password & Registry Editor available at http://pogostick.net
- Windows Password Reset Kit available at http://www.reset-windows-password.net
- Windows Password Recovery Tool available at http://www.windowspasswordsrecovery.com
- ElcomSoft System Recovery available at http://www.elcomsoft.com
- Trinity Rescue Kit available at http://trinityhome.org
- Windows Password Recovery Bootdisk available at http://www.rixler.com
- PasswordLastic available at http://www.passwordlastic.com
- Stellar Phoenix Password Recovery available at http://www.stellarinfo.com

- Windows Password Recovery Personal available at http://www.windows-passwordrecovery.com
- Windows Administrator Password Reset available at http://www.systoolsgroup.com

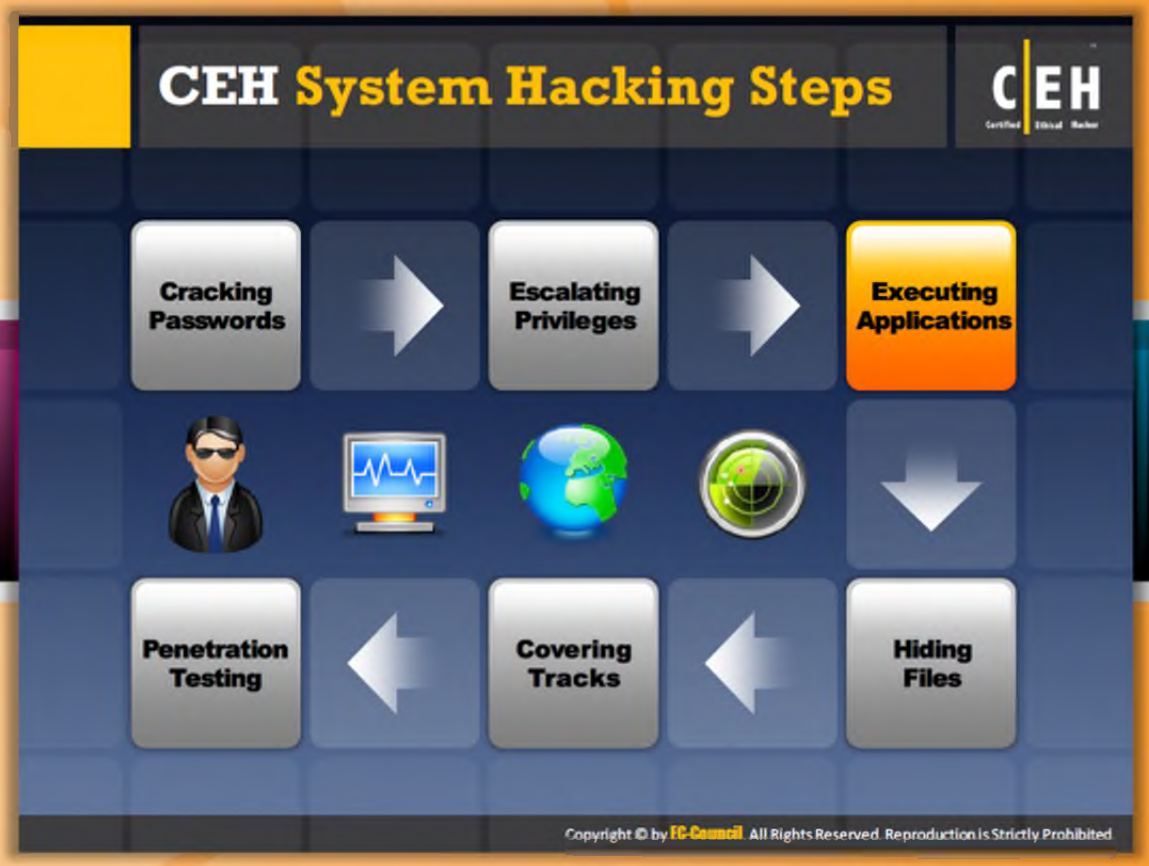
How to Defend against Privilege Escalation

The **best countermeasure** against privilege escalation is to ensure that users have the least possible privileges or just enough privileges to use their system effectively. Often, **flaws in programming code** allow such escalation of privileges. It is possible for an attacker to gain access to the network using a **non-administrative** account. The attacker can then gain the **higher privilege** of an administrator.

General privilege escalation countermeasures include:

- Restrict the interactive logon privileges
- Run users and applications on the **least privileges**
- Implement multi-factor authentication and authorization
- Run services as **unprivileged** accounts
- Use encryption technique to protect **sensitive data**
- Implement a privilege separation methodology to limit the scope of programming errors and bugs
- Reduce the amount of **code** that runs with particular privilege

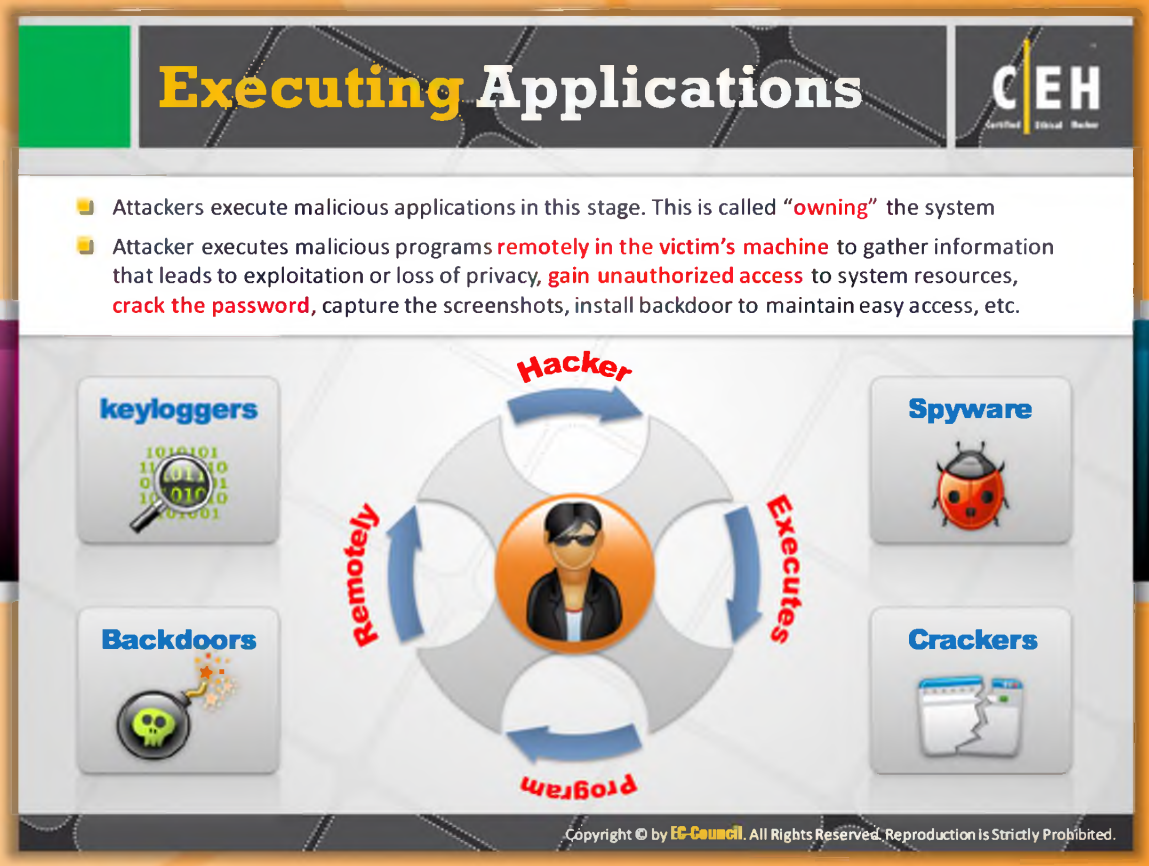
- Perform debugging using bounds checkers and stress tests
- Test operating system and application coding errors and bugs thoroughly
- Patch the systems regularly



CEH System Hacking Steps

By executing a **malicious application** on the victim system, an attacker could exploit a vulnerability to execute arbitrary code with **higher privileges** than they would otherwise have been allowed. By executing malicious applications, the attacker can **steal personal information**, gain unauthorized access to the system resources, crack passwords, **capture screenshots**, install a **backdoor** for maintaining easy access, etc. Detailed explanation about executing applications is as follows.

Cracking Passwords	**Hiding Files**
Escalating Privileges	**Covering Tracks**
Executing Applications	**Penetration Testing**

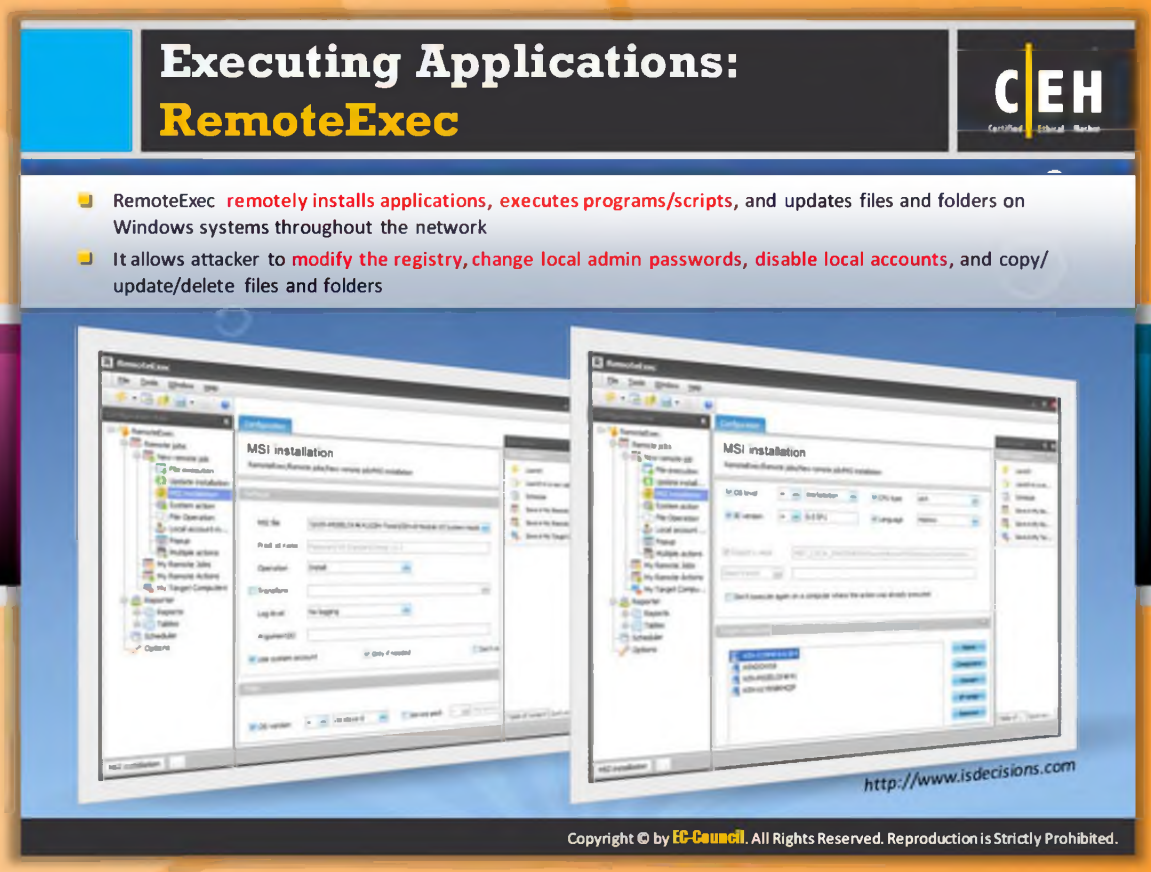


Executing Applications

Attackers execute malicious applications in this stage. This is called "owning" the system. Executing applications is done after the attacker gains the **administrative privileges**. The attacker may try to execute some of his or her own malicious programs 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, etc. The malicious programs that the attacker executes on victim's machine may be:

- **Backdoors** - Programming 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 the purpose of **cracking the code** or passwords.
- **Keyloggers** - This can be hardware or a software type. In either case the objective is to record each and every keystroke made on the computer keyboard.
- **Spyware** - Spy software may capture the **screenshots** and send them to a **specified location** defined by the hacker. The attacker has to maintain the access to the victim's computer until his or her purpose is fulfilled. After **deriving** all the requisite information

from the victim's computer, the attacker installs several backdoors to maintain easy access to the **victim's computer** in the future.



Executing Applications: RemoteExec

Source: http://www.isdecisions.com

RemoteExec allows you to remotely install applications and execute **programs/scripts** all over the network. Any file and folder can be updated, copied, as well as deleted instantaneously on **Windows systems**. With the help of this the attacker can change the Local Administrator Password remotely and can **disable** all other local accounts for **reinforcing security**. In addition, it can also reboot, shut down, wake up, and power off a **computer remotely**.

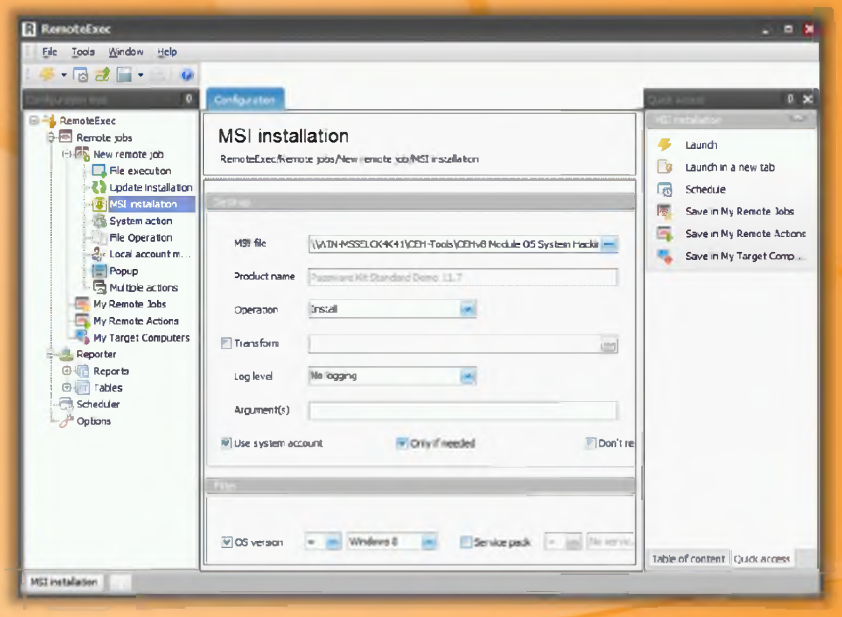


FIGURE 5.27: RemoteExec Screenshot

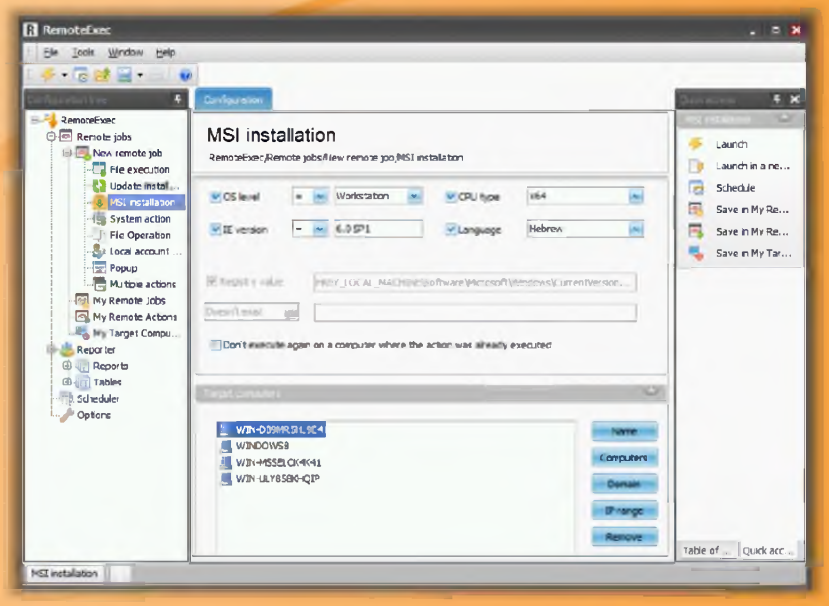


FIGURE 5.28: RemoteExec in Target Computers Screenshot

Executing Applications: PDQ Deploy

Source: http://www.adminarsenal.com

PDQ Deploy is a software deployment tool with which you can easily install almost any application or patch to your computer. MSI, MSP, MSU, EXE and **batch installers** can be remotely deployed to numerous Windows computers at the same time using this **tool**. You can easily and quickly deploy a **packaged** program to the selected or to all computers on your network quickly. 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, etc.

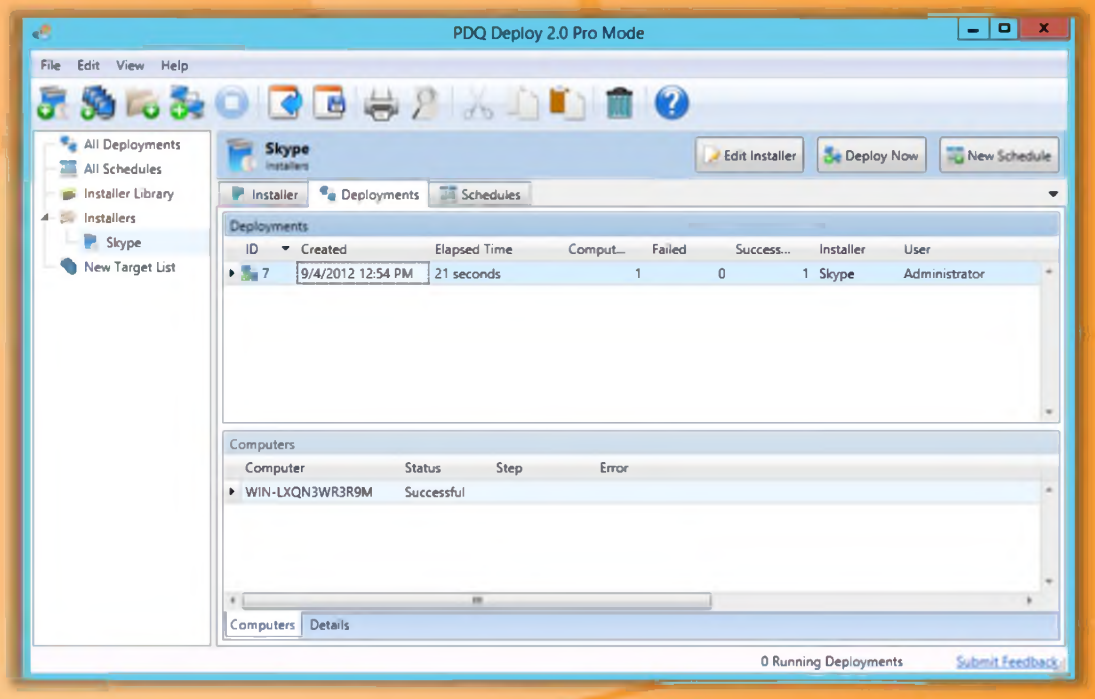
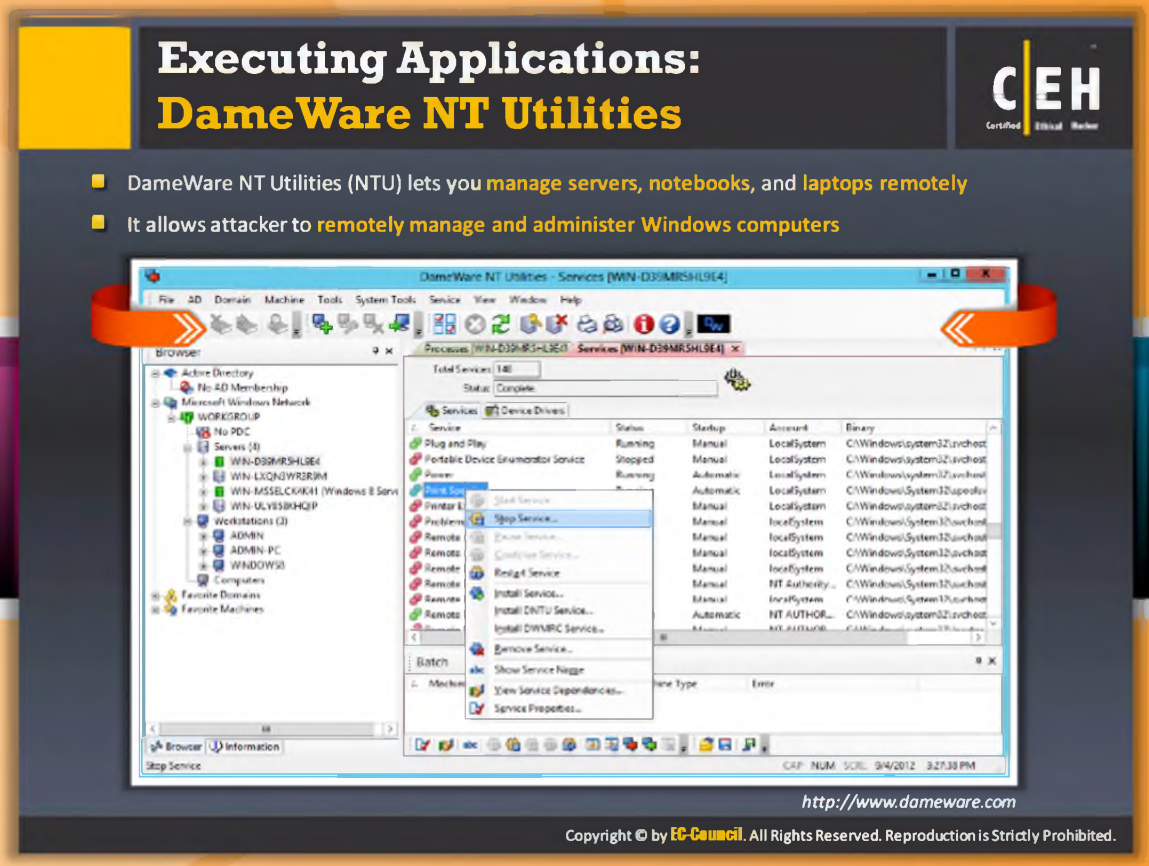


FIGURE 5.29: PDQ Display Screenshot



Executing Applications: DameWare NT Utilities

Source: http://www.dameware.com

DameWare NT Utilities allows you to manage servers, notebooks, and laptops remotely. With the help of this, you can manage and administer **Windows computers remotely**. It has the capability of solving end-user problems using a **remote control**. It can reboot the servers and notebooks remotely, take screenshots of remote desktops, take full control of the end-user's desktop quickly, copy as well as **delete files** on the remote computers, manage **Windows Active** Directory, etc.

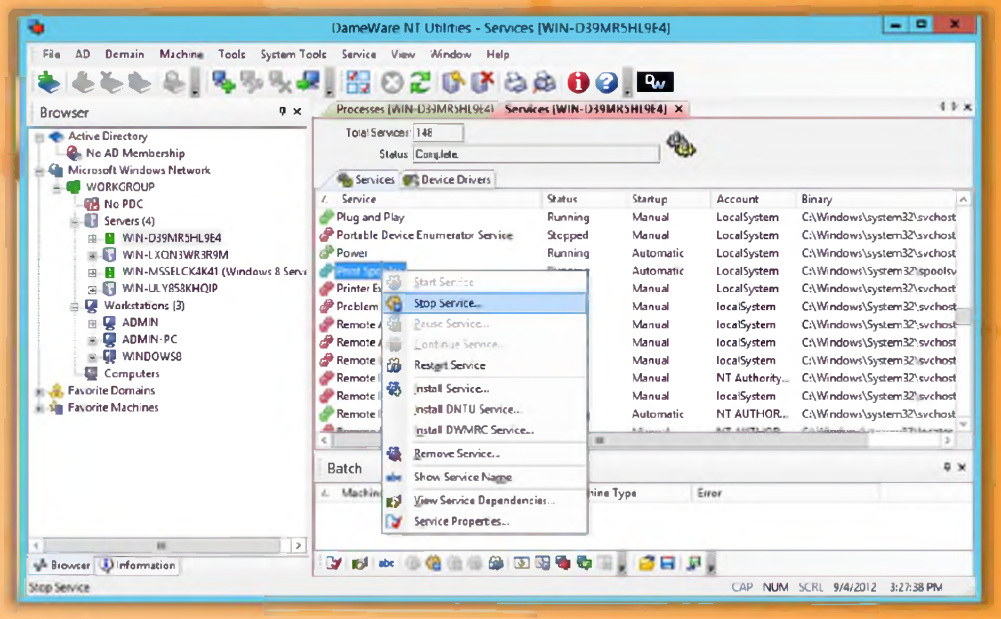
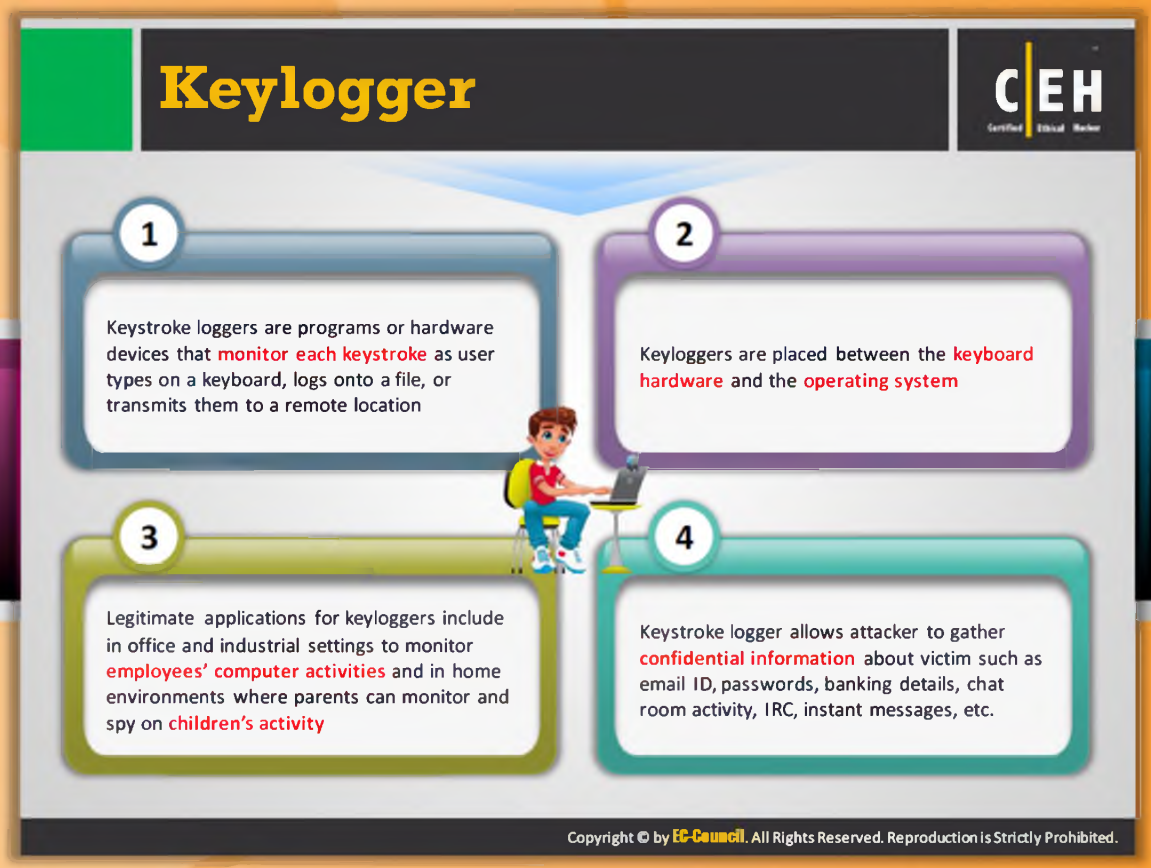


FIGURE 5.30: DameWare NT Utilities Screenshot



Keyloggers

Keyloggers, also called keystroke logging, are software programs or **hardware devices** that record the keys struck on the computer keyboard of an individual computer user or network of computers. You can view all the **keystrokes** that are typed at any time in your system by **installing** this hardware device or programs. It records almost all the keystrokes that are typed by a user and saves the recorded information in a text file. As it is convert, the person does not know that their activities are being **monitored**. It is mostly used for positive purposes such as in offices and **industrial settings** for monitoring the employees' computer activities and in home environments where parents can monitor what their children are doing on the Internet.

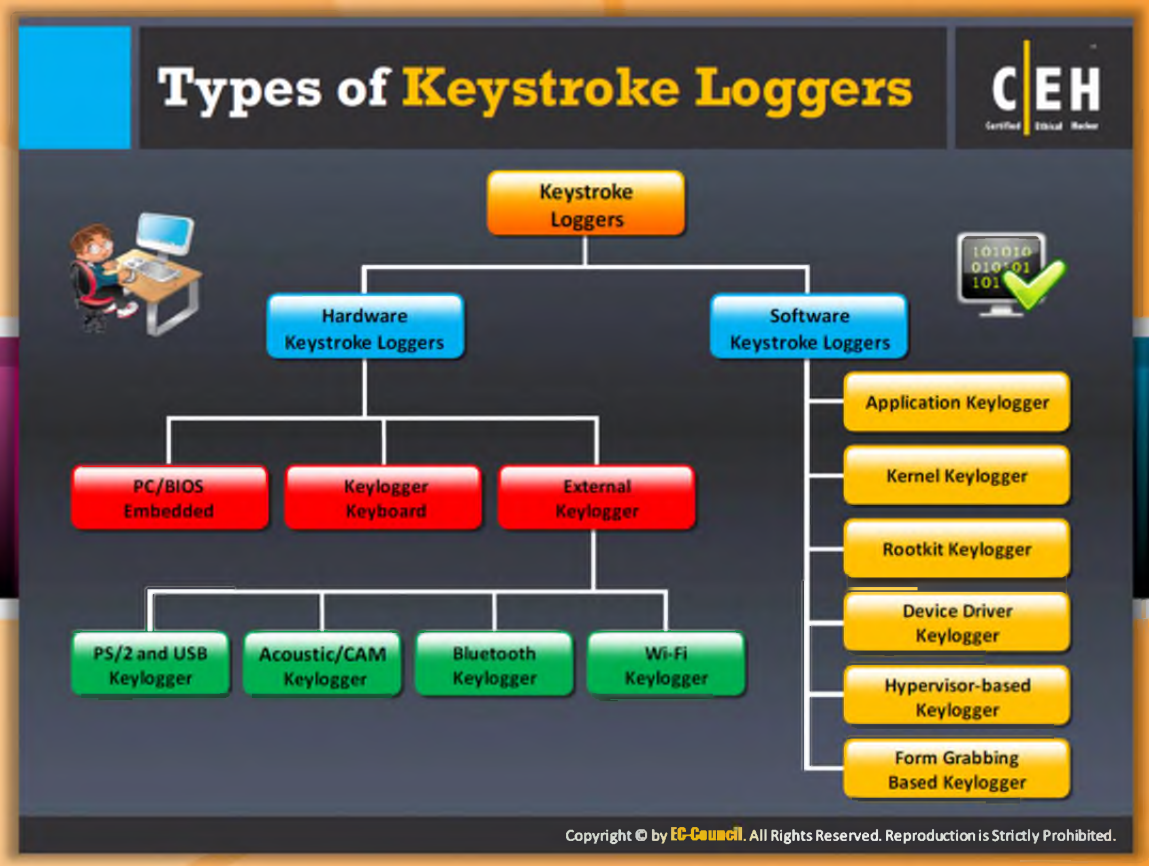
A keylogger, when associated with spyware, helps to transmit your information to an unknown third party. It is used **illegally** by attackers for malicious purposes such as for stealing sensitive and confidential information about victims. The **sensitive information** includes email IDs, passwords, banking details, chat room activity, IRC, instant messages, bank and credit card numbers, and other information that is typed by people every day. The data, i.e., transmitted over the encrypted Internet connection, is also vulnerable to **keylogging** because the keylogger tracks the keys struck before they are **encrypted** for **transmission**.

The keylogger program is installed onto the user's system invisibly through email attachments or through "drive-by" downloads when users visits certain websites. Keystroke loggers are

stealth software that sits between **keyboard hardware** and the operating system, so that they can record every keystroke.

A keylogger can:

- Record each keystroke, i.e., typed by the user, on his or her computer keyboard.
- Capture screenshots at regular intervals of time showing user activity such as when he or she types a character or clicks a mouse button.
- 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 that they have visited and with the keywords entered by them, etc.
- Record all the login names, bank and credit card numbers, and passwords including hidden passwords or data that are in asterisks or blank spaces.
- Record online chat conversations.
- Make **unauthorized copies** of both **outgoing email** messages and incoming email messages.



Types of Keystroke Loggers

A keylogger is a small software program that records each and every keystroke that is typed by the user at any time on a specific computer's keyboard. The captured keystrokes are saved in a file for reading later or otherwise **transmitted** to a place where the attacker can access it. As this programs records all the keystrokes that are typed through a keyboard, they can capture the passwords, credit card numbers, email address, names addresses, and phone numbers. **Keyloggers** have the **ability to capture information** before it can be **encrypted** for transmission over the network. This gives the attacker access to **pass phrases** and other well-hidden information.

There are two types of keystroke loggers. They are hardware loggers and software loggers. These **two loggers** are used for **recording** all the **keystrokes** that are entered on a system on which they are installed.

Hardware Loggers

Hardware keyloggers are hardware devices look like normal USB drives. It is connected between a keyboard plug and **USB socket**. All the recorded keystrokes that are typed by the user are stored within a hardware unit. Attackers retrieve this hardware unit for accessing the **keystrokes** that are stored in it. The **primary advantage** of these **loggers** is that

they cannot be detected by antispyware, antivirus, or desktop security programs. Its disadvantage is that its physical presence can be easily discovered.

Hardware keystroke loggers are classified into **three main types**:

PC/BIOS Embedded

Physical and/or admin-level access is necessary to the computer, and the application loaded into the computer's BIOS must be made for the particular hardware that it will be running on. BIOS-level firmware that manages keyboard actions can be modified to capture these events as they are processed.

Keylogger Keyboard

These keyloggers are used for recording keyboard events by attaching a hardware circuit with the keyboard's cable connector. It records the all the keyboard strokes to its own internal memory that can be accessed later. The main advantage of a hardware keylogger over a software keylogger 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 that are typed by the user on the computer keyboard, and store the data such as emails, chat records, applications useds, IMs, etc.
- **Acoustic/CAM Keylogger** – Makes use of either a capturing receiver capable of **converting** the **electromagnetic sounds** into the **keystroke data** or a CAM that is capable of recording screenshots of the keyboard.
- **Bluetooth Keylogger** – Requires physical access to the target computer only once, at the time of installation. Once this is installed on the **target PC**, it stores all the keystrokes and you **can retrieve** the keystrokes information in real time by connecting through a Bluetooth device.
- **Wi-Fi Keylogger** – **Operates** completely stand alone. Unlike a Bluetooth keylogger, this kind of keylogger doesn't require it be near the computer on which the dongle (recording device in Bluetooth keylogger) is installed to retrieve the keystroke information. This keylogger requires no software or drivers and is completely undetectable; it works on any PC. This records the **keystrokes** and sends the information by **email** over a **predefined** time interval.

Software Keystroke Loggers

These loggers are the software installed remotely via a network or email attachment in the computer for recording all the keystrokes that are typed on the computer keyboard. Here the logged information is stored as a log file in a hard drive of the computers. Physical access is not required on the part of the person probing to obtain keystroke data because data is emailed out from the machine at **predetermined intervals**. Software loggers often have the ability to obtain much additional data as well, since they are not limited by physical memory allocations as are hardware keystroke loggers. Software keystroke loggers are classified into **six types**. They are:

- Application Keylogger
- Kernel Keylogger
- Rootkit Keylogger
- Device Driver Keylogger
- Hypervisor-based Keylogger
- Form-Grabbing-Based Keylogger

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 a completely **invisible keylogger** to track and record everything happening within the entire network.

Kernel Keylogger

This method is used rarely because it is difficult to write as it requires a high level of **proficiency** from the developer of the keylogger. It is also difficult to conflict. 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 the information typed on the keyboard.

Rootkit Keylogger

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 tools or dedicated tools.

Device Driver Keylogger

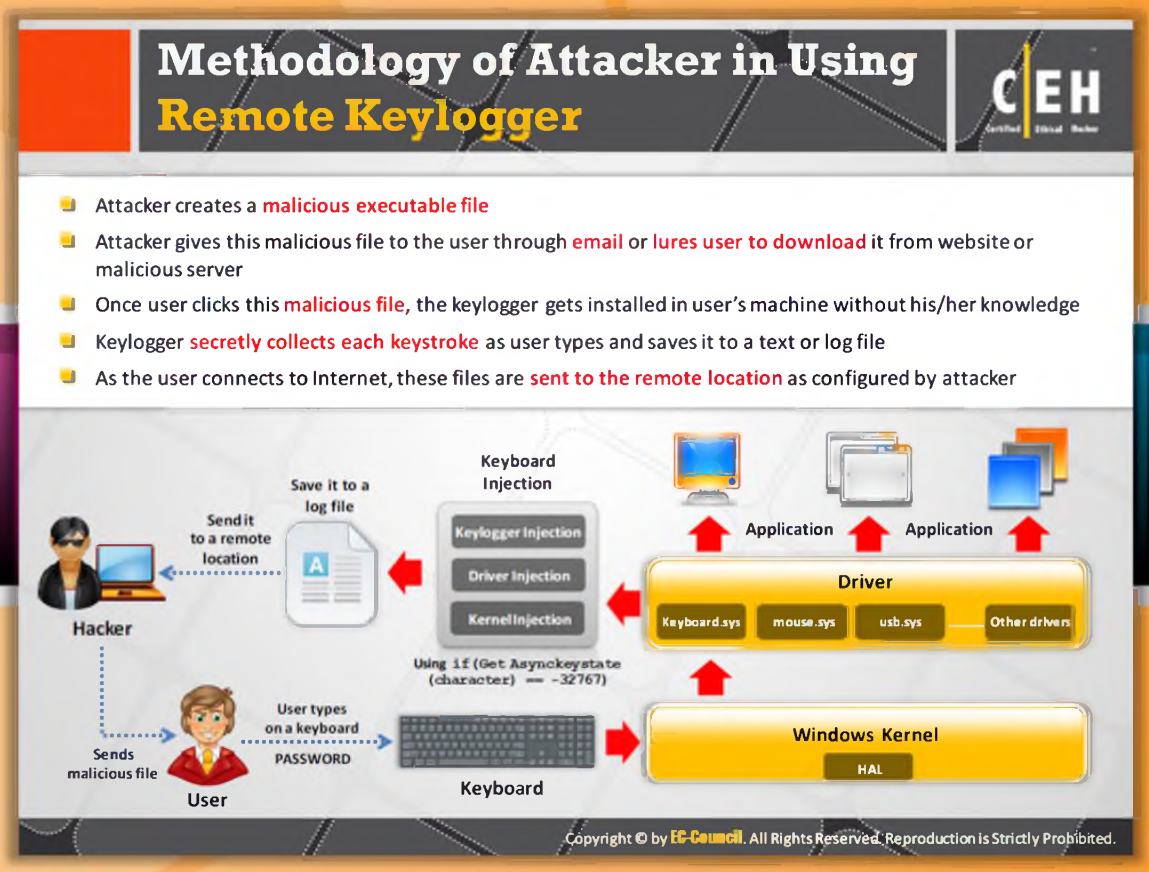
This kind of keylogger usually acts as a device driver. The device driver keylogger replaces the existing I/O driver with the embedded keylogging functionality. All the keystrokes performed on the computer are saved into a hidden logon file and then it is sent to the **destination** through the Internet. The **log files** sent to the destination by this keylogger are hidden and it is tough to distinguish from the operating system files, even while doing a directory listing of hidden files.

Hypervisor-based Keylogger

A hypervisor-based keylogger is built within a malware hypervisor operating underneath the operating system and cannot be physically seen or touched. They are the same as virtual machines.

FormGrabber-Based Keylogger

In a form-grabbing-based keylogger, the web form data is recorded first and then after it is submitted over the Internet, it bypasses https encryption. Form-grabbing-based keyloggers log web form inputs by recording web browsing on the Submit event function.



Methodology of Attacker in Using Remote Keylogger

For viewing the data remotely, the attacker first creates a malicious executable file and sending this **malicious file** to the victim through email (i.e., hiding the malicious file behind the genuine file, like an image or song), or otherwise lures the user to download it from a website or **malicious server**. Once the victim clicks this malicious file, the keylogger is installed on the victim system and the **victim** does not know that this keylogger software is installed on his or her system as it is **invisible** to the victim. The keylogger secretly collects each keystroke that is typed by the user and saves it to a text or log file. The **log file** may contain **sensitive information** such as bank account numbers and passwords, credit card numbers, phone numbers, addresses, etc. As the victim connects to the Internet, these files are sent to the remote location as configured by the attacker. Here the attacker does not need to have physical access to the victim's machine.

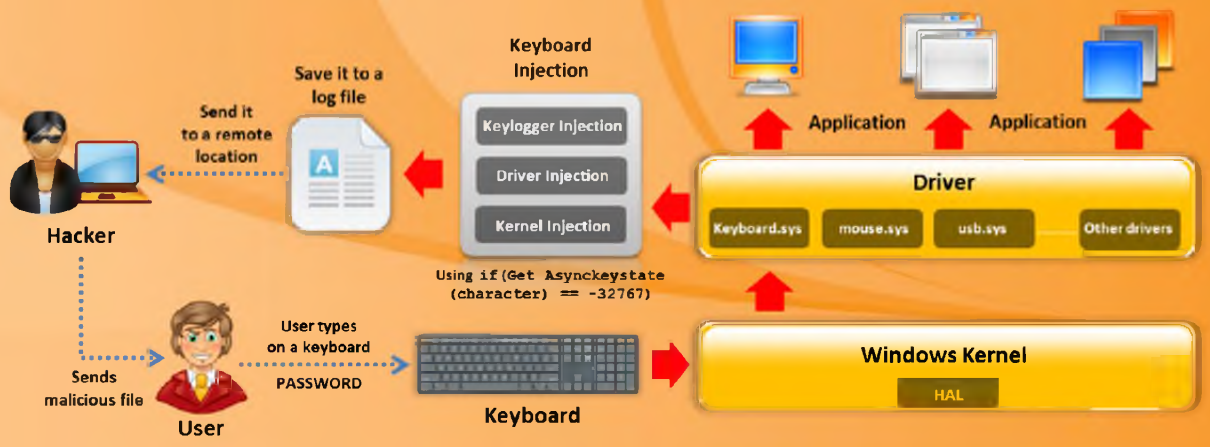
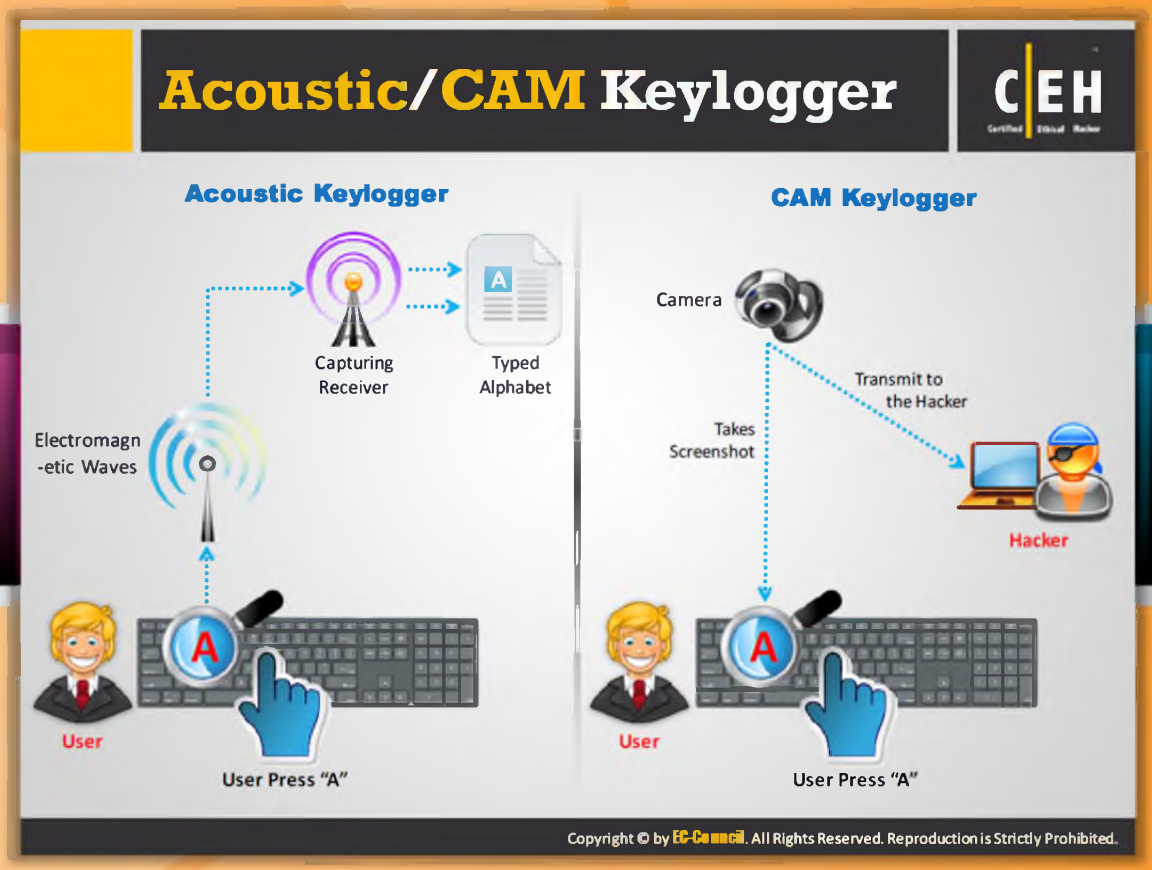


FIGURE 5.31: Methodology of Attacker in Using Remote Keylogger



Acoustic/CAM Keyloggers

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 what is being typed by the user.

The acoustic keylogger requires a "learning period" of 1,000 or more keystrokes to convert the recorded sounds into the data. This is done by applying a frequency algorithm to the recorded sounds. To determine which sound corresponds to which key, the acoustic keylogger uses statistical data based on the frequency with which each key is used because some letters will be used much more than others.

FIGURE 5.32: Acoustic Keyloggers

A **CAM keylogger** makes use of the webcam to record the keystrokes. The cam installed takes screenshots of the keystrokes and the monitor and sends the recorded screenshots to the attacker account at **periodical intervals**. The attacker can retrieve the keystroke information by probing the **screen shots** sent by the CAM keylogger.

FIGURE 5.32: CAM Keyloggers

Keyloggers

Beside the information discussed previously, **acoustic/CAM** keyloggers, there are other **external keyloggers** that you can use to monitor the keystrokes of someone's system. These external keyloggers can be attached between a **usual PC keyboard** and a computer to record each keystroke.

You can use following **external hardware** keyloggers to **monitor** user activity:

FIGURE 5.33: Different Types of Keyloggers

Keylogger: Spytech SpyAgent

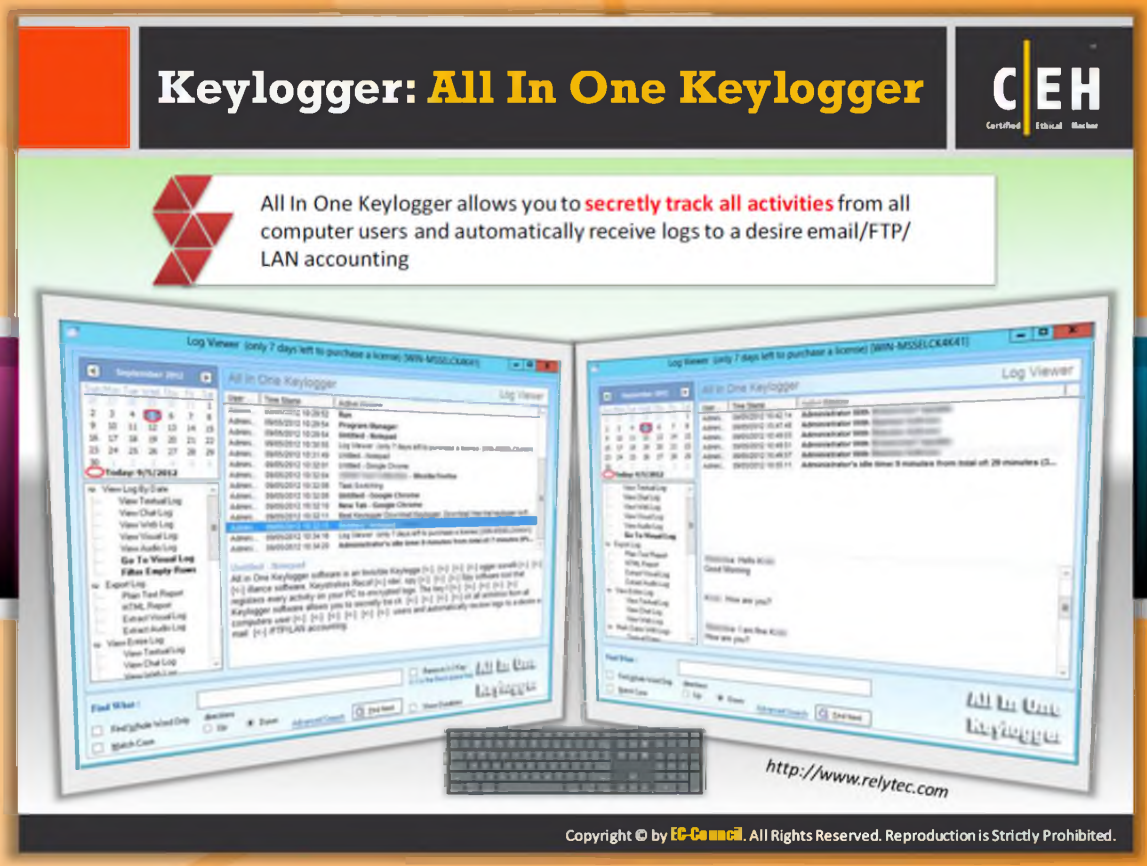
Source: http://www.spytech-web.com

Spytech SpyAgent is software keystroke logger that allows you to monitor the **keystrokes** of the user computer on which it is installed. It can also allow you to **monitor** following things on a user computer:

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

You can download this software keylogger from its home site and install it on the computer you want to monitor, and then just click **Start Monitoring**. That's it! It will record a number of things for you about user activity on the computer.

FIGURE 5.34: SpyAgent Screenshot



Keylogger: All In One Keylogger

Source: http://www.relytec.com

All In One Keylogger is invisible keylogger **surveillance** software that allows you to record keystrokes and **monitors** each **activity** of the user on the computer. It allows you to **secretly track** all activities from all computer users and automatically receive logs to a desired **email/FTP/LAN** account. The keylogger automatically activates itself when Windows starts and is completely invisible. You can do following things using this software:

- 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
- **Captured** screenshots
- Send reports by FTP
- Send reports in HTML format
- Block unwanted URLs
- Stop logging when the computer is idle

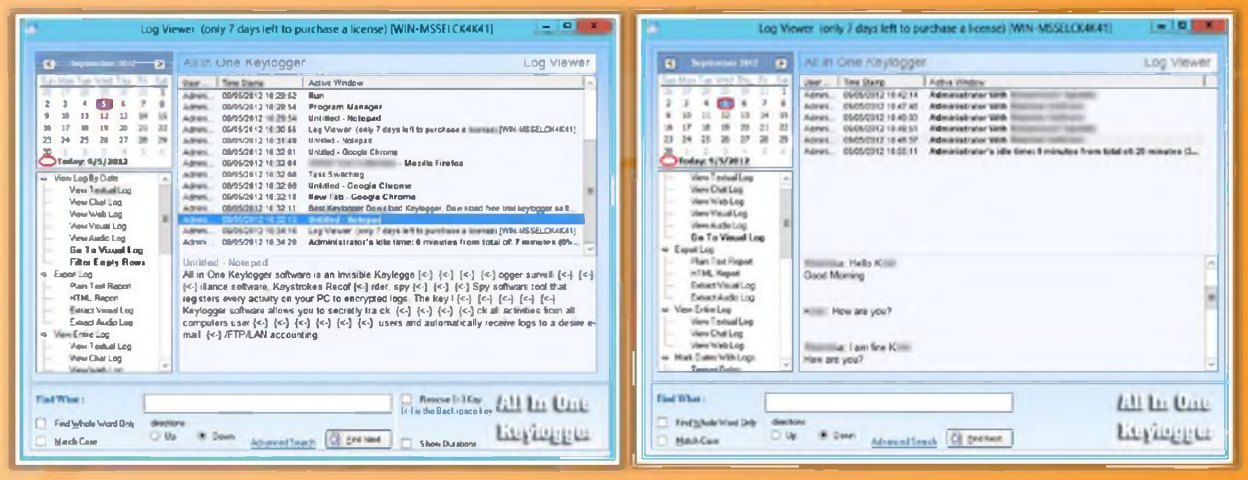


FIGURE 5.35: All In One Keylogger Screenshot

Keyloggers for Windows

Besides the **keyloggers** explained previously, there are so many software keyloggers available in the market; you can make use of these tools to record the **keystrokes** and **monitor** each activity of the user on the computer. These keyloggers are listed as follows. They all are used to record the keystrokes on the user computer. You can download these tools from their respective home sites as follows and start using them to **monitor keystrokes** and other user activity on the computer.

Here is the list of keyloggers that run on the Windows operating system:.

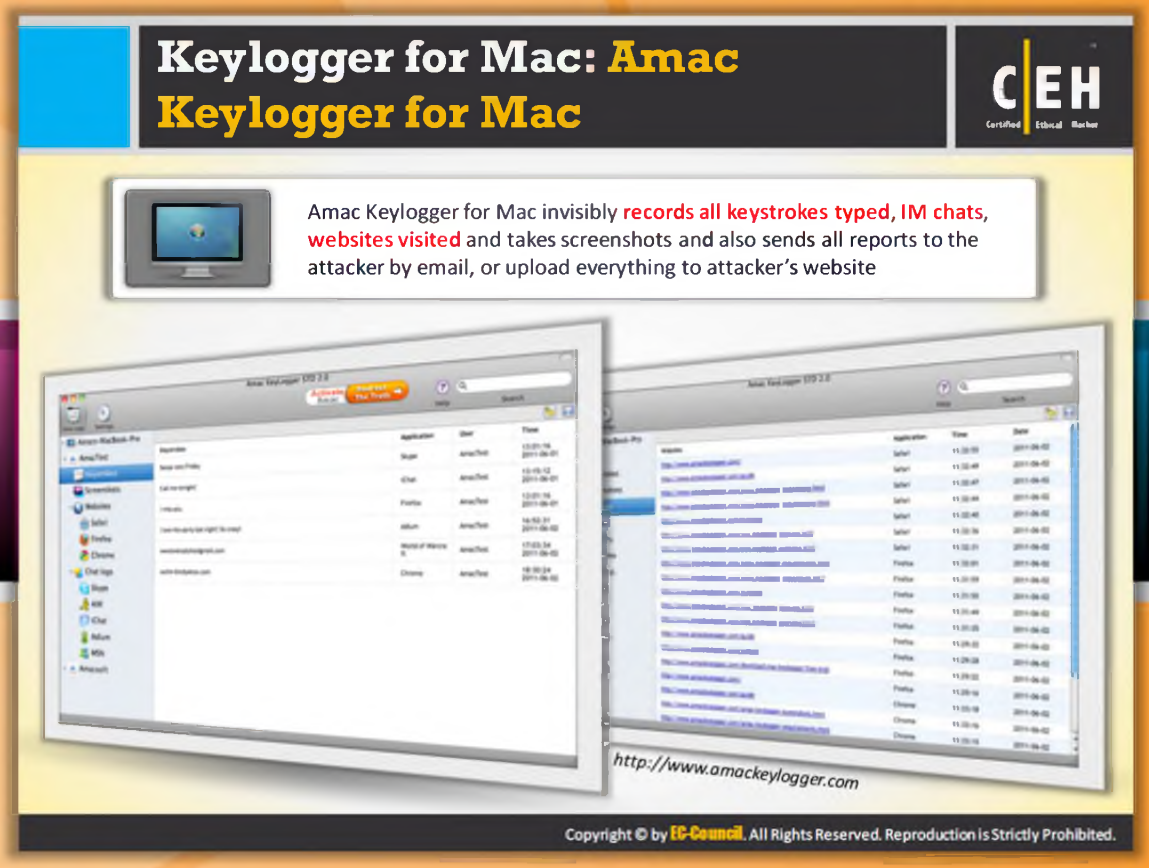
- Ultimate Keylogger available at http://www.ultimatekeylogger.com
- Advanced Keylogger available at http://www.mykeylogger.com
- The Best Keylogger available at http://www.thebestkeylogger.com
- SoftActivity Keylogger available at http://www.softactivity.com
- Elite Keylogger available at http://www.widestep.com
- Powered Keylogger available at http://www.mykeylogger.com
- StaffCop Standard available at http://www.staffcop.com
- iMonitorPC available at http://www.imonitorpc.com

- PC Activity Monitor Standard available at http://www.pcacme.com
- KeyProwler available at http://keyprowler.com

Keyloggers for Windows

You can also use following keyloggers that runs on the **Windows operating system**:

- Keylogger Spy Monitor available at http://ematrixsoft.com
- REFOG Personal Monitor available at http://www.refog.com
- Actual Keylogger available at http://www.actualkeylogger.com
- Spytector available at http://www.spytector.com
- KidLogger available at http://kidlogger.net
- PC Spy Keylogger available at http://www.pc-spy-keylogger.com
- Revealer Keylogger available at http://www.logixoft.com
- Spy Keylogger available at http://www.spy-key-logger.com
- Actual Spy available at http://www.actualspy.com
- SpyBuddy® 2012 available at http://www.exploreanywhere.com



Keylogger for Mac: Amac Keylogger for Mac

Source: http://www.amackeylogger.com

Amac Keylogger is a keylogger that runs on **Mac operating systems** and allows you to spy on a Mac machine to secretly record everything on the Mac. It does the following things:

- **Log typed passwords**
- **Log keystrokes** and chat conversations
- Record websites and take screenshots
- Log the IP address of the **monitored** Macintosh
- Automatically run at startup stealthily
- Apply settings to all users with one click
- Send logs to email/FTP at preset intervals
- Password **protect** keylogger access

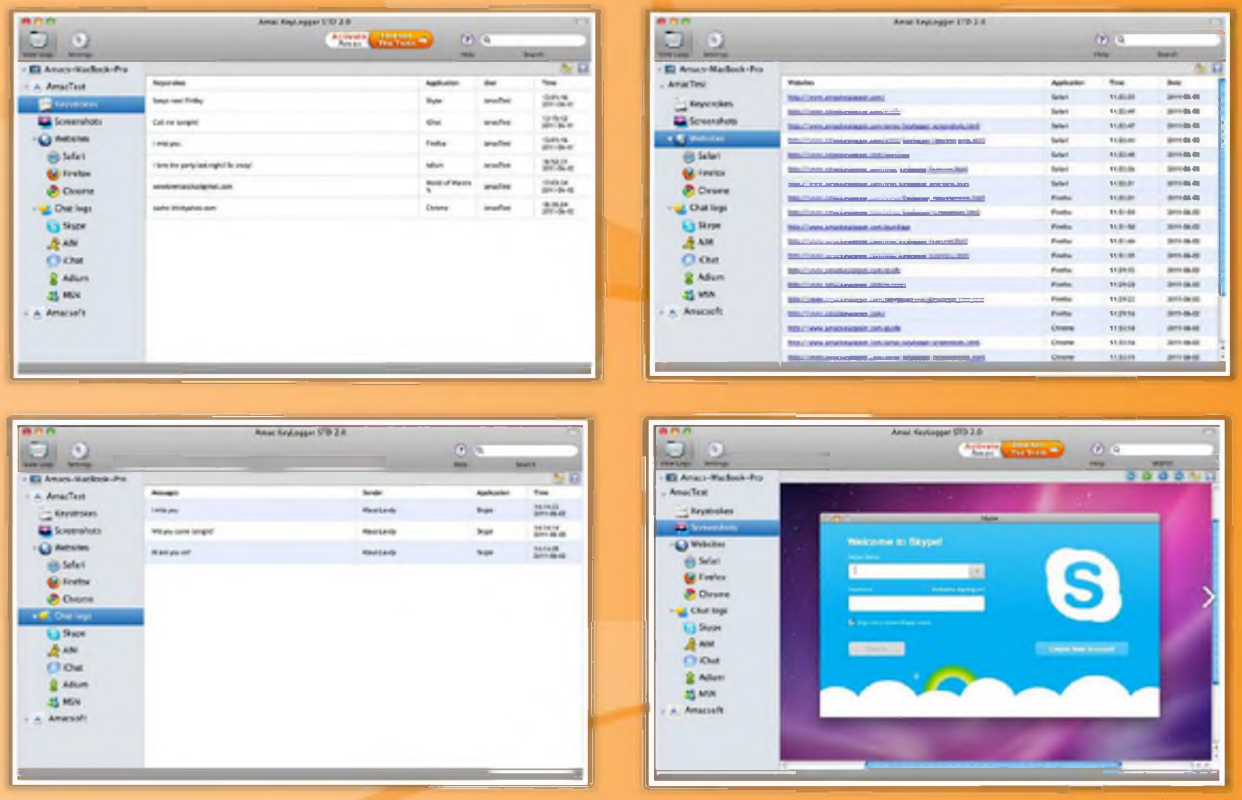
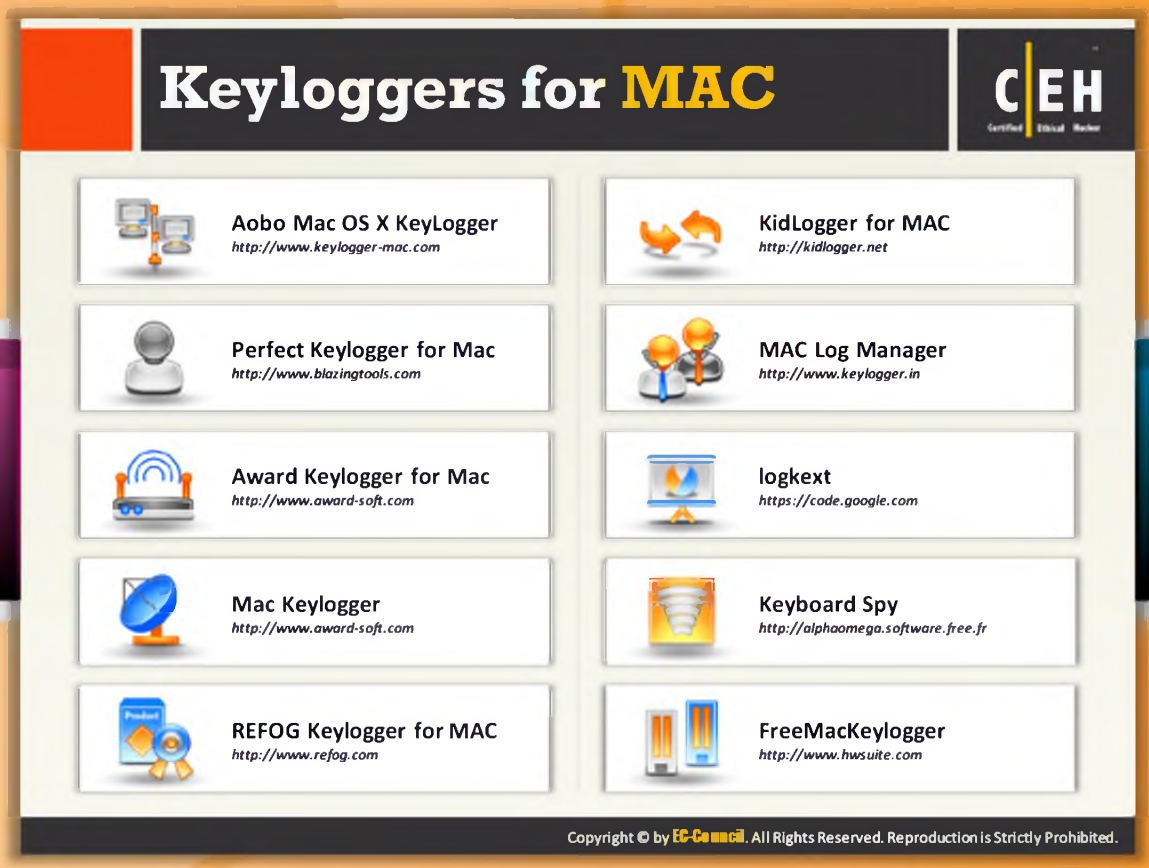


FIGURE 5.36: Amac Keylogger for Mac



Keyloggers for Mac

Like keyloggers for Windows, there are also many keyloggers that runs on the **Mac operating system**. These tools will assist you in recording **keystrokes** and **monitoring** the user activity on the target MAC OS computer system. You can download them from their respective home sites and they can be used to spy on a Mac machine to **secretly record** everything on the Mac. 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, etc.

You can use the following keystroke loggers for Mac OS:

- Aobo Mac OS X KeyLogger available at http://www.keylogger-mac.com
- Perfect Keylogger for Mac available at http://www.blazingtools.com
- Award Keylogger for Mac available at http://www.award-soft.com
- Mac Keylogger available at http://www.award-soft.com
- REFOG Keylogger for MAC available at http://www.refog.com
- KidLogger for MAC available at http://kidlogger.net
- MAC Log Manager available at http://www.keylogger.in

- logkext available at https://code.google.com
- Keyboard Spy available at http://alphaomega.software.free.fr
- FreeMacKeylogger available at http://www.hwsuite.com

Hardware Keyloggers

A hardware keylogger is a device that is connected in between a **keyboard** and the **computer**. It is used to record the keystrokes on the target user computer. Hardware keyloggers log all keyboard activity to their internal memory. The advantage of a hardware keylogger over software keyloggers is they it can log the keystrokes as soon as the **computer starts**. You can use following hardware keystroke loggers to **achieve your goals**.

KeyGhost

Source: http://www.keyghost.com

KeyGhost is a tiny plug-in device that records every keystroke typed on any computer. You can also monitor and **record** email communication, chatroom activity, instant messages, website addresses, search engine searches, and more with this **plug-in** keylogger. You do not have to install any software to record or **retrieve keystrokes**.

Features:

- It is easy to use
- Installs in seconds; just plug it in
- Can be unplugged and information retrieved on another PC

- Uses no system resources
- Excellent real-time backup device

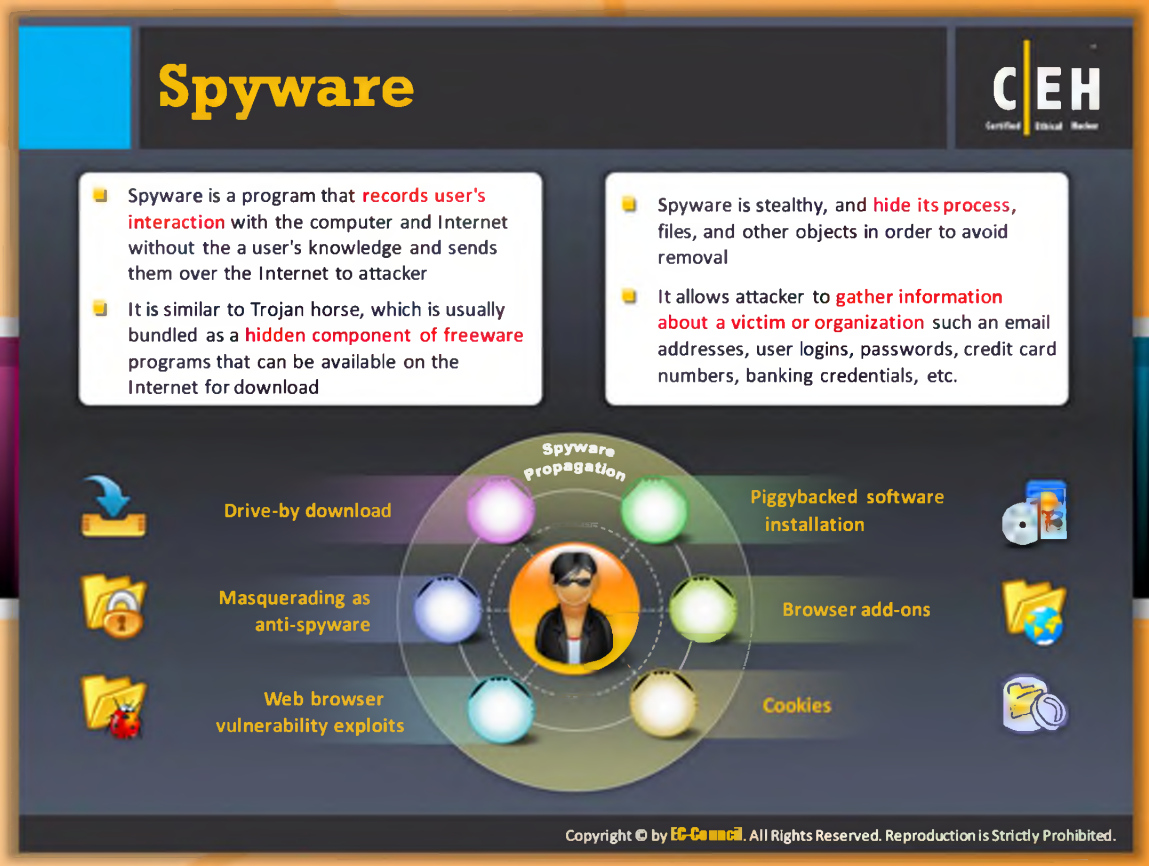
FIGURE 5.37: KeyGhost Screenshot

KeyGrabber

Source: http://www.keydemon.com

KeyGrabber is a hardware device that allows you to log keystrokes from a PS/2 or USB keyboard. A **hardware video-logger** is a tiny frame-grabber for capturing **screenshots** from a VGA, DVI, or HDMI video source.

FIGURE 5.37: KeyGrabber Screenshot



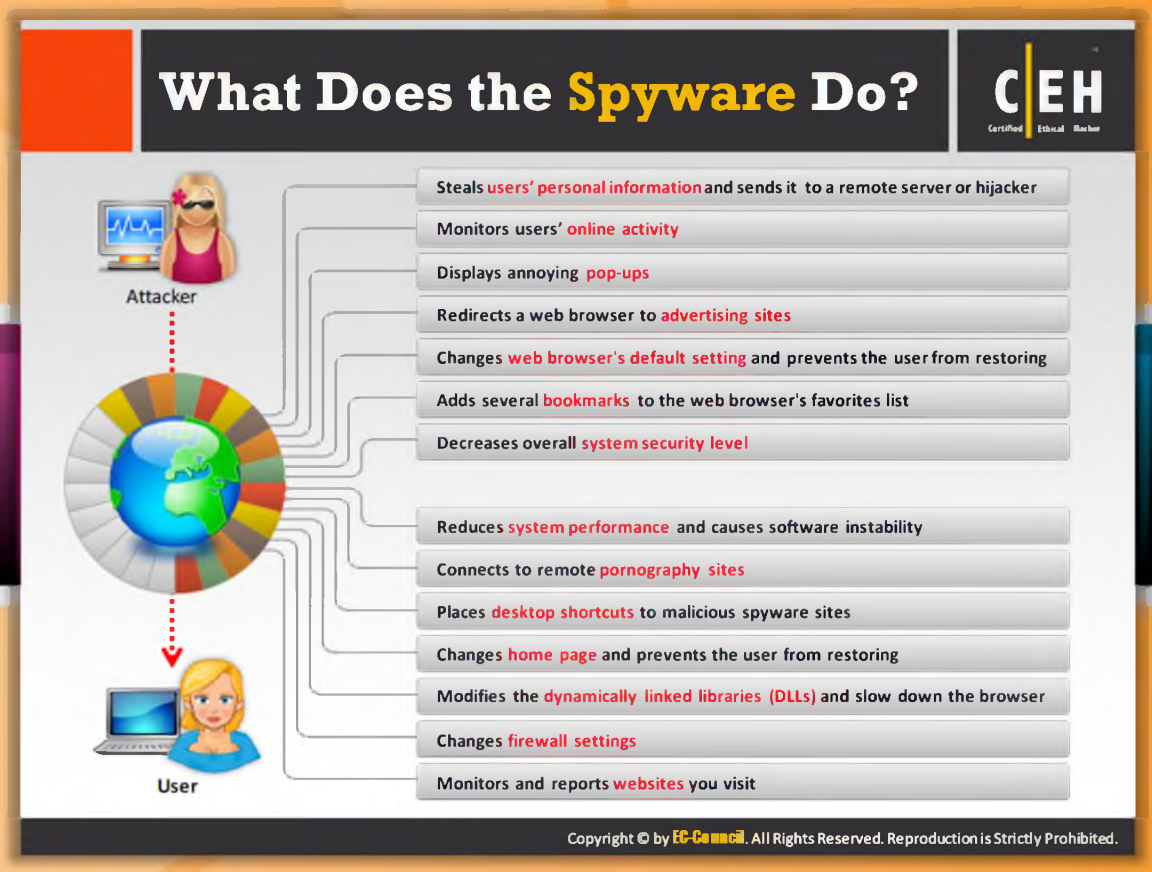
Spyware

Spyware is **stealthy computer monitoring software** that allows you to secretly record all activities of a computer user. It automatically delivers logs to you 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 directly pointed at the computer monitor. **Spyware** is usually bundled as a hidden component of freeware or shareware programs that can be **downloaded** from the Internet.

Spyware Propagation

Installing the spyware on the user's computer doesn't require any consent from the user. You can install the **spyware** on the user's computer without their knowledge by "**piggybacking**" the spyware on other software programs. This is possible because spyware uses advertising cookies, which is one of the **spyware subclasses**. You can also be affected by spyware when you visit a website that distributes spyware. This is sometimes called "**drive-by downloading**" since it installs itself when you "drive by" the website.

Because of a lack of user's attention in downloading and installing applications from the Internet, it is possible that the spyware is installed. The spyware **propelled** with other programs on the Internet **masquerade** as **antispyware** and run on the user's computer without any notice, when the user downloads and installs programs that are **bundled with spyware**.

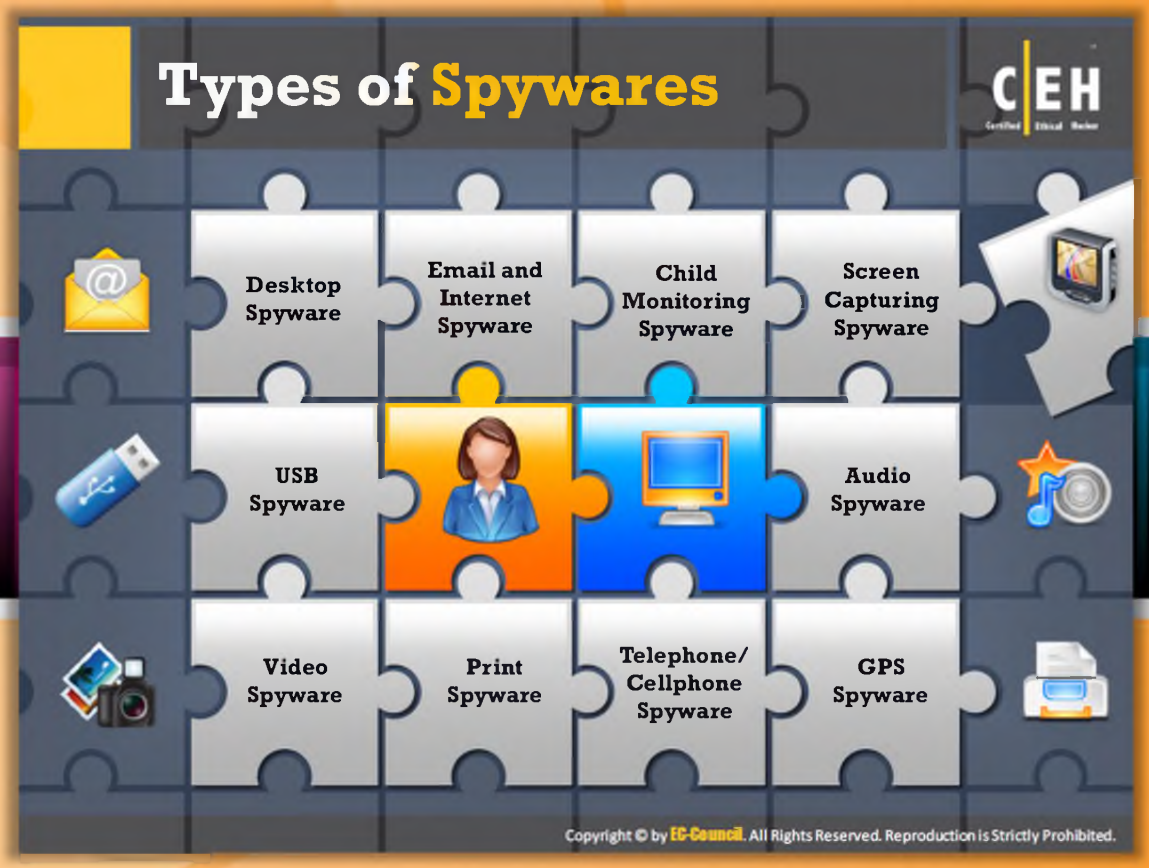


What Does the Spyware Do?

Once you have succeeded in **installing spyware** on a **victim's computer**, you can do many offensive things to the victim's computer. You can do following things with spyware installed on the victim's computer:

- Steals users' personal information and send it to a remote server or hijacker
- Monitor users' online activity
- Display annoying pop-ups and **redirect** a web browser to advertising sites
- Change web browser's default setting and prevent the user from restoring
- Add multiple **bookmarks** to the web browser's favorites list
- Decrease overall system security level
- Place desktop shortcuts to malicious spyware sites
- Connect to remote **pornography** sites
- Reduce system performance and causes software instability
- Steal your passwords
- Send you **targeted** email

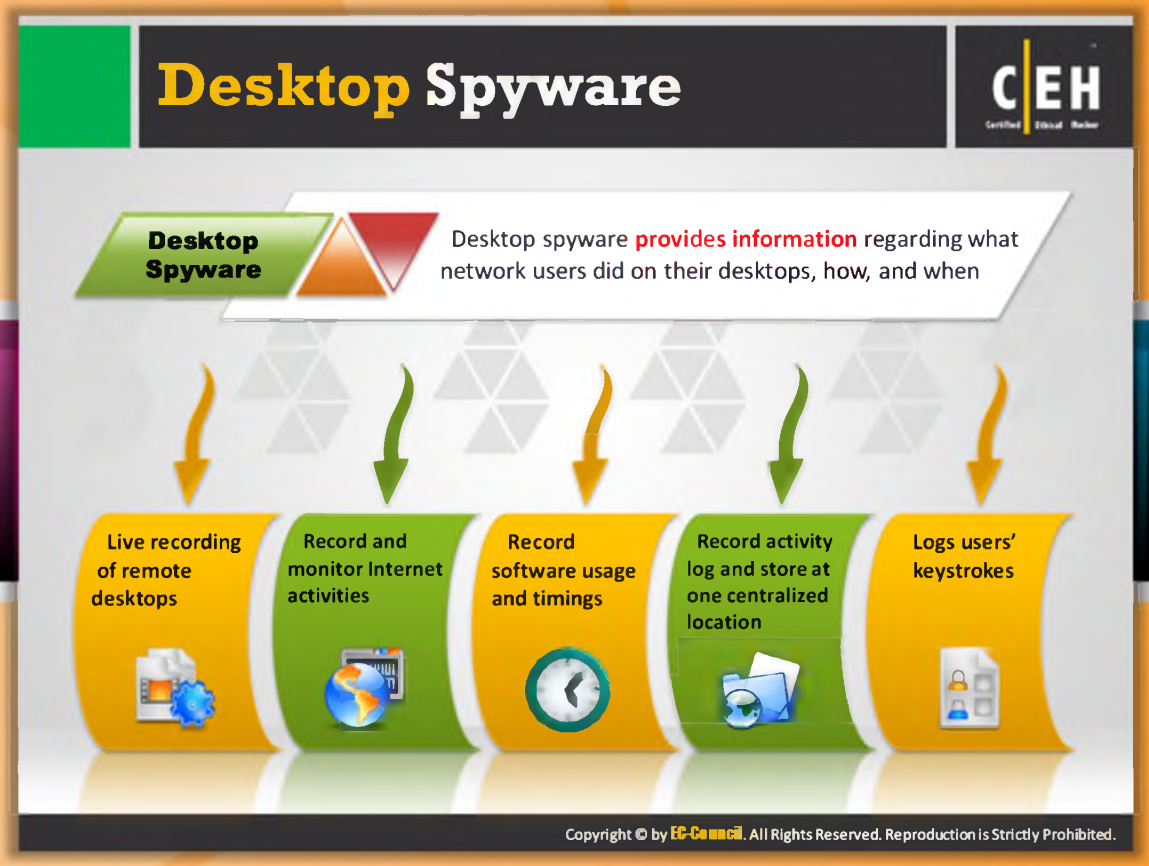
- Change the home page and prevent the user from restoring:
- Modifie the **dynamically linked libraries** (DLLs) and slow down the browser
- Change firewall settings
- **Monitor** and **report** websites you visit



Types of Spyware

There are **10 main types** of **spyware operating** on the Internet that an attacker can use to steal information about user activity on computer without his/her consent and knowledge. The following are these 10 types:

- Desktop Spyware
- Email and Internet Spyware
- Child **Monitoring** Spyware
- Video Spyware
- Print Spyware
- Screen **Capturing** Spyware
- USB Spyware
- Audio Spyware
- GPS Spyware
- Cell Phone and Telephone Spyware

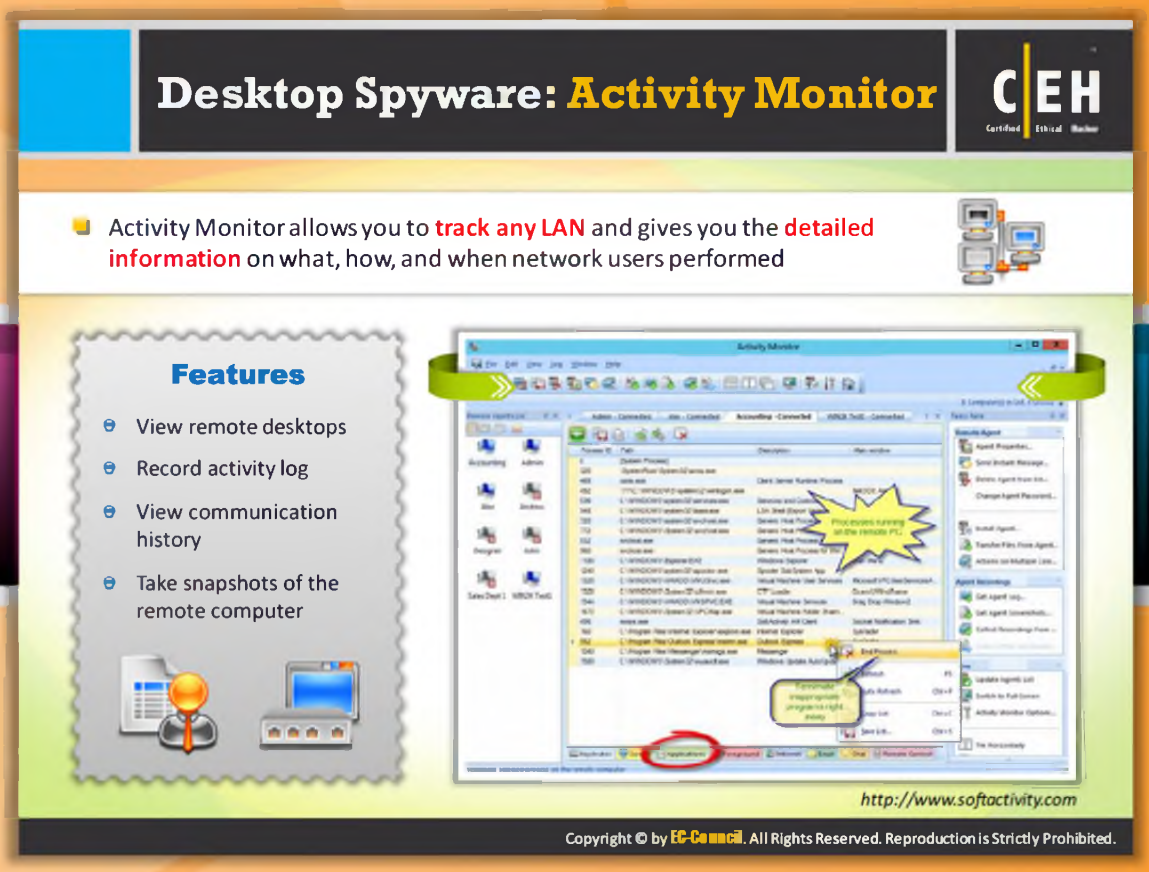


Desktop Spyware

Desktop spyware is software that allows an attacker to gain information about a user's activities 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
- **Record and monitor** Internet activities
- Record software usage and timings
- Record activity log and store at one centralized location
- Logs users' keystrokes



Desktop Spyware: 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. **Activity Monitor Server** can be installed on any computer in the whole **LAN**. Remote spy software is installed on all computers on the network that you want to monitor. Remote spy software is also known as the Agent, a small client program. Agent can be installed remotely from the PC with Activity Monitor Server on it or via **Active Directory Group Policy** in Windows domain.

Any computer in the network under control can be spied on remotely 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 on the network.

Features:

- Live view of remote desktops (screenshot)
- Easy Internet usage monitoring
- Monitor software usage

- Record activity log for all workplaces in one **centralized** location on a main computer with Activity Monitor installed
- Store complete history of **communications** for every user (emails sent and received, IM chats, messages typed in web forums)
- Track any user's keystrokes, even passwords on your screen, in real-time mode
- Total control over networked computers. Start or terminate remote processes, run commands, copy files from remote systems. You may even turn the computer off or restart it, not to mention **logging** off the current user
- Deploy Activity Monitor Agent (the client part of the software) remotely from the administrator's PC to all computers in your network

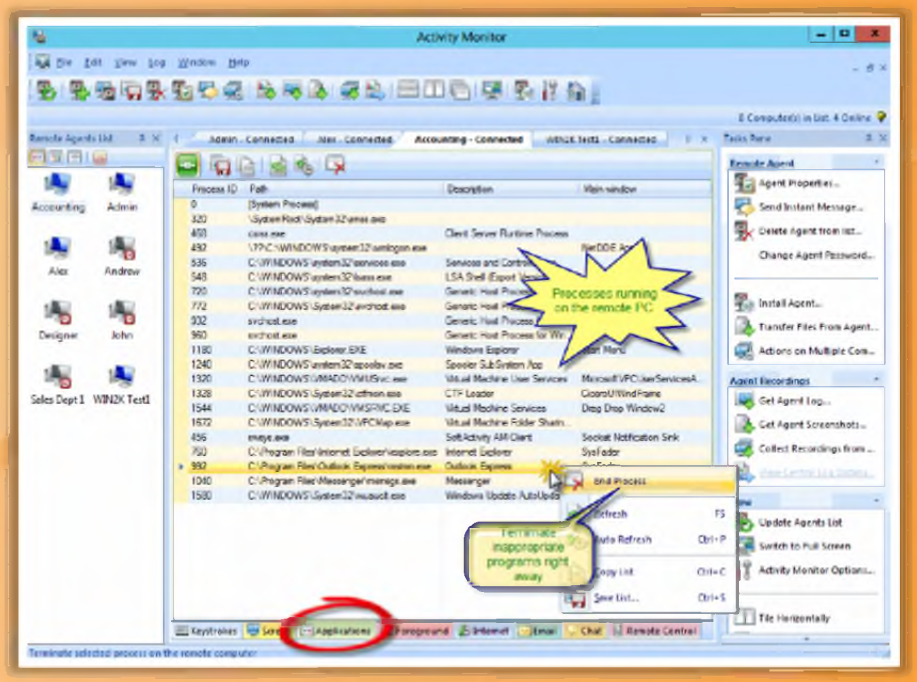
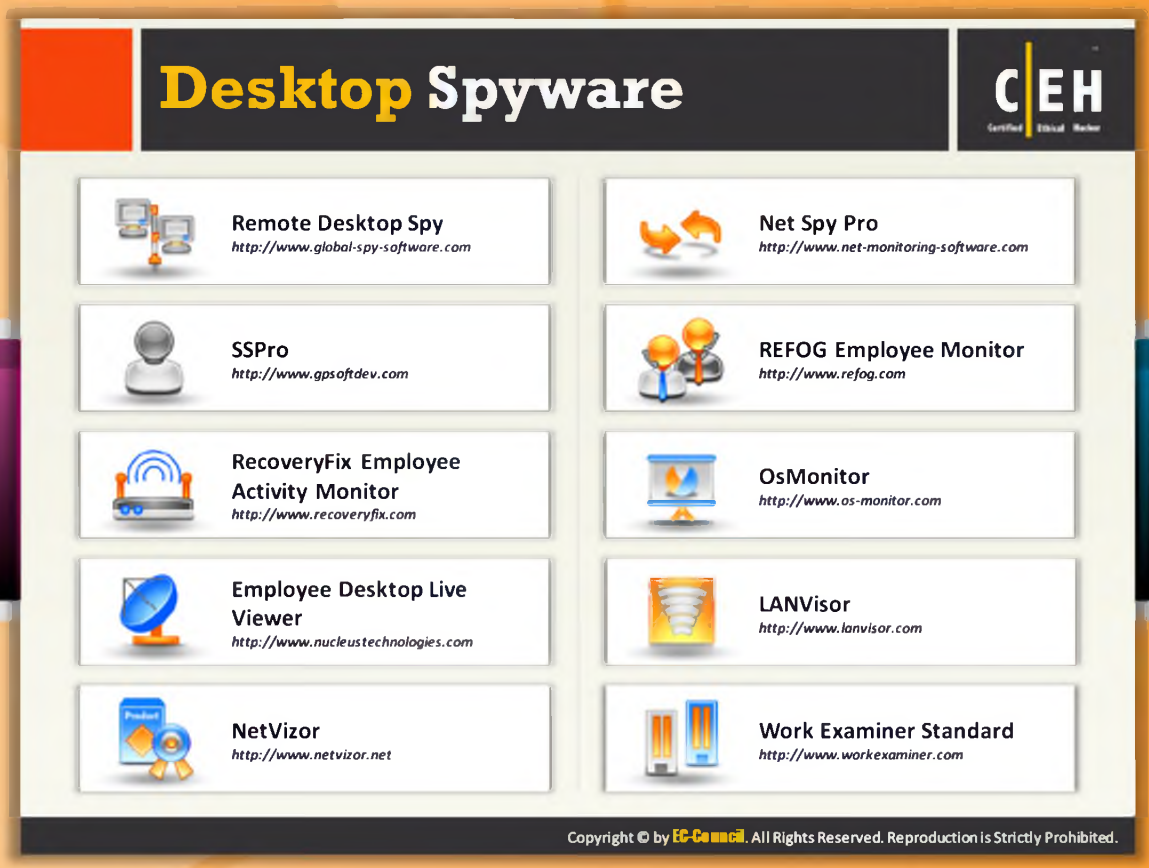


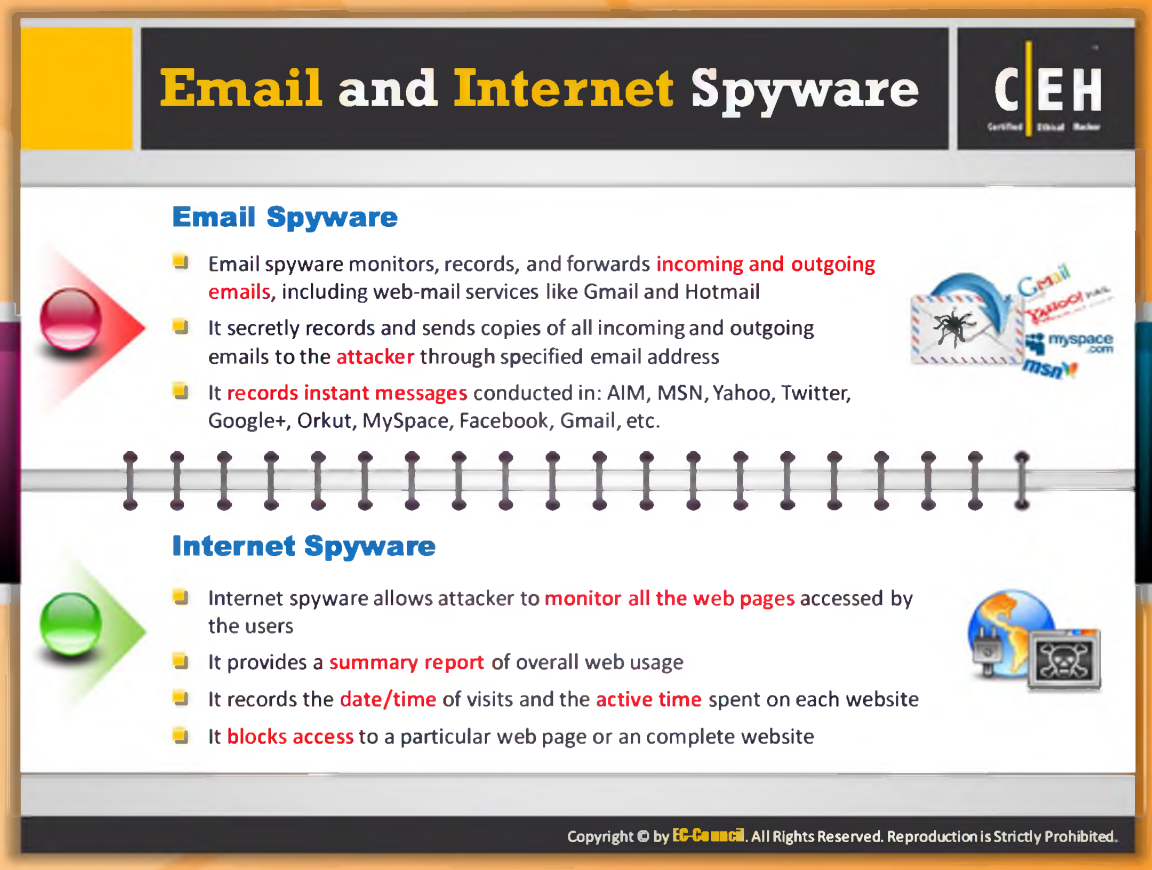
FIGURE 5.38: Desktop Spyware by Using Activity Monitor



Desktop Spyware

There is various **desktop spyware** available in the market that an attacker can use to monitor remote user desktops. This spyware can be used to monitor and **record** every detail of user PC and Internet activity. An attacker can log keystrokes, websites visited by the user, programs running on the user computer, chat conversations, email communication, downloaded files, opened/closed windows, etc. You can also take **snapshots** of the remote user desktop and much more. Some of desktop spyware software that attackers may use for **monitoring** user desktops remotely are listed as follows:

- Remote Desktop Spy available at http://www.global-spy-software.com
- SSPro available at http://www.gpsoftdev.com
- RecoveryFix Employee Activity Monitor available at http://www.recoveryfix.com
- Employee Desktop Live Viewer available at http://www.nucleustechnologies.com
- NetVizor available at http://www.netvizor.net
- Net Spy Pro available at http://www.net-monitoring-software.com
- REFOG Employee Monitor available at http://www.refog.com
- OsMonitor available at http://www.os-monitor.com
- LANVisor available at http://www.lanvisor.com
- Work Examiner Standard available at http://www.workexaminer.com



Email and Internet Spyware

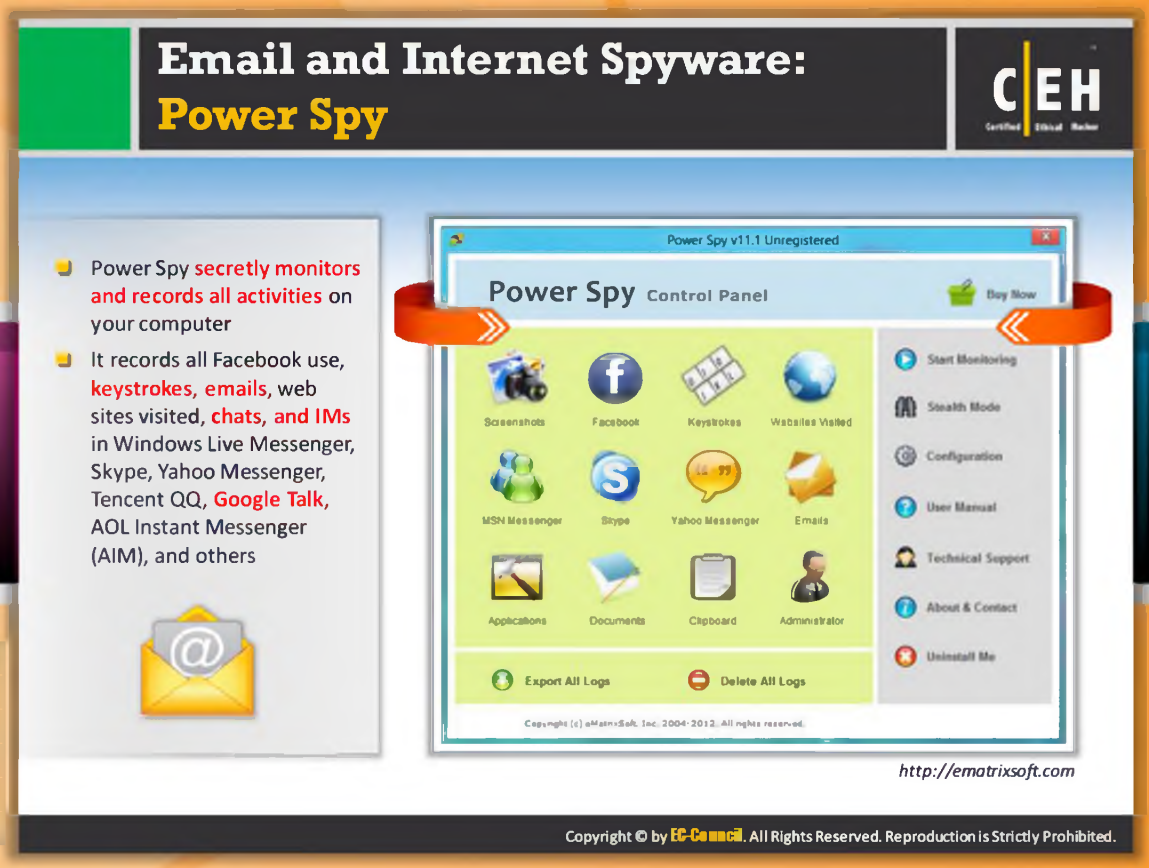
Email Spyware

Email spyware is a program or software that monitors, records, and forwards all incoming and outgoing emails, including **webmail services** such as Hotmail and Yahoo mail. 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 on the local disk folder of the **monitored** computer. This works in a stealth mode; the users on the computer will not be aware of the presence of email spyware on their computer. It is also capable of recording **instant messages** conducted in: AIM, MSN, Yahoo, MySpace, Facebook, etc.

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. It runs in **stealth mode**, which means it runs in the background and the users on your computer can never detect this tool is installed on the computer. All the visited **URLs** are written into a log file and sent to a specified email address. Using Internet spyware, one can perform web **activity surveillance** on any computer. 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 **mentioning the URLs** or the keywords that you want to block on your computer.



Email and Internet Spyware: Power Spy

Source: http://ematrixsoft.com

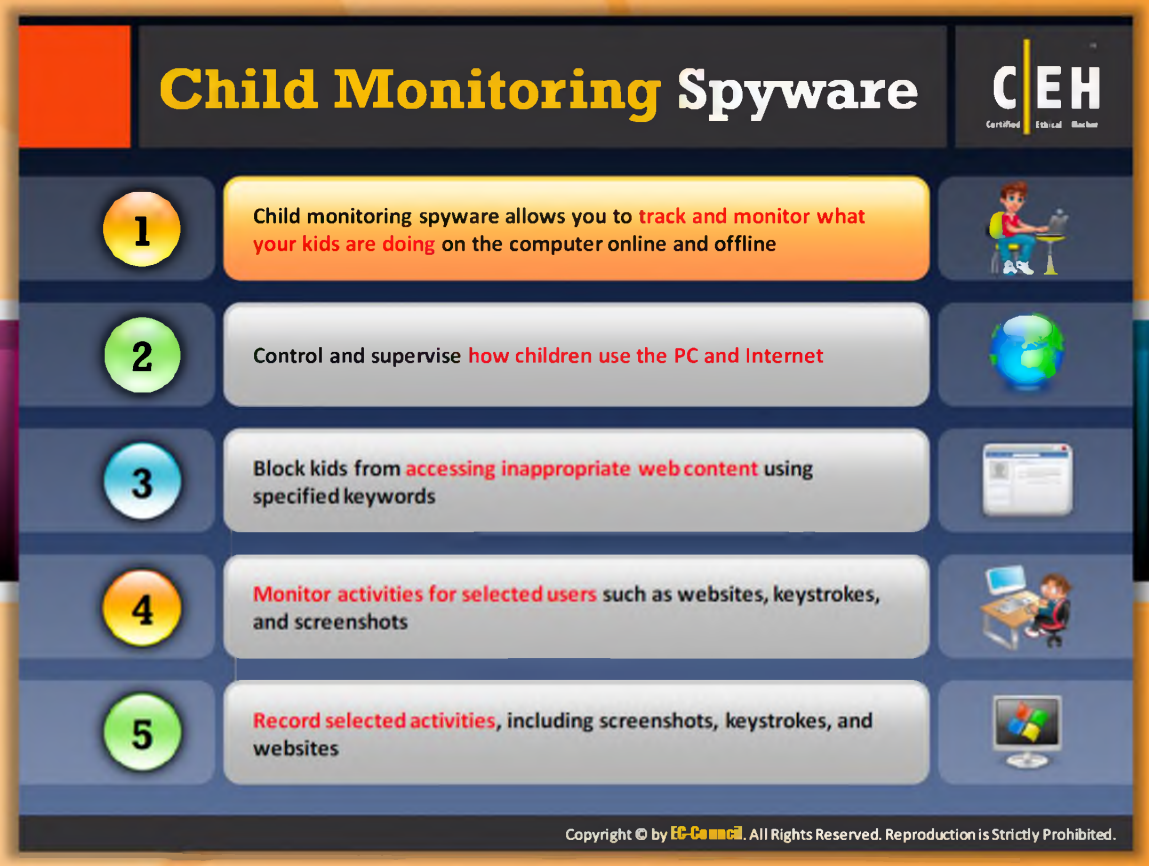
Power Spy software allows you to **monitor** your computer from a remote place whenever you are away from the PC. It records all Facebook use, keystrokes, emails, web sites visited, chats & IMs in Windows Live Messenger (MSN Messenger), Skype, Yahoo Messenger, Tencent QQ, Google Talk, GADU-GADU, ICQ, AOL Instant Messenger (AIM), and more. In addition, it even records clipboard data, passwords typed, documents opened, windows opened, and applications executed. It starts **automatically** with system startup, runs secretly, and sends log reports to your **email** or **FTP**. You can check these **reports** anywhere you like.

FIGURE 5.39: Email and Internet Spyware by Using Power Spy

Internet and Email Spyware

Internet and email Spyware records as well as reviews all activities such as emails, instant messages, andkeystrokes on computers, tablets, and mobile phones. It even protects your family from danger online and **safeguards** your **company** from **risk** and **loss**. A fFew Internet and email spyware programs are listed as follows:

- eBLASTER available at http://www.spectorsoft.com
- Imonitor Employee Activity available at http://www.employee-monitoring-software.cc
- Employee Monitoring available at http://www.employeemonitoring.net
- OsMonitor available at http://www.os-monitor.com
- Ascendant NFM available at http://www.ascendant-security.com
- Spylab WebSpy available at http://www.spylab.org
- Personal Inspector available at http://www.spyarsenal.com
- CyberSpy available at http://www.cyberspysoftware.com
- AceSpy available at http://www.acespy.com
- EmailObserver available at http://www.softsecurity.com

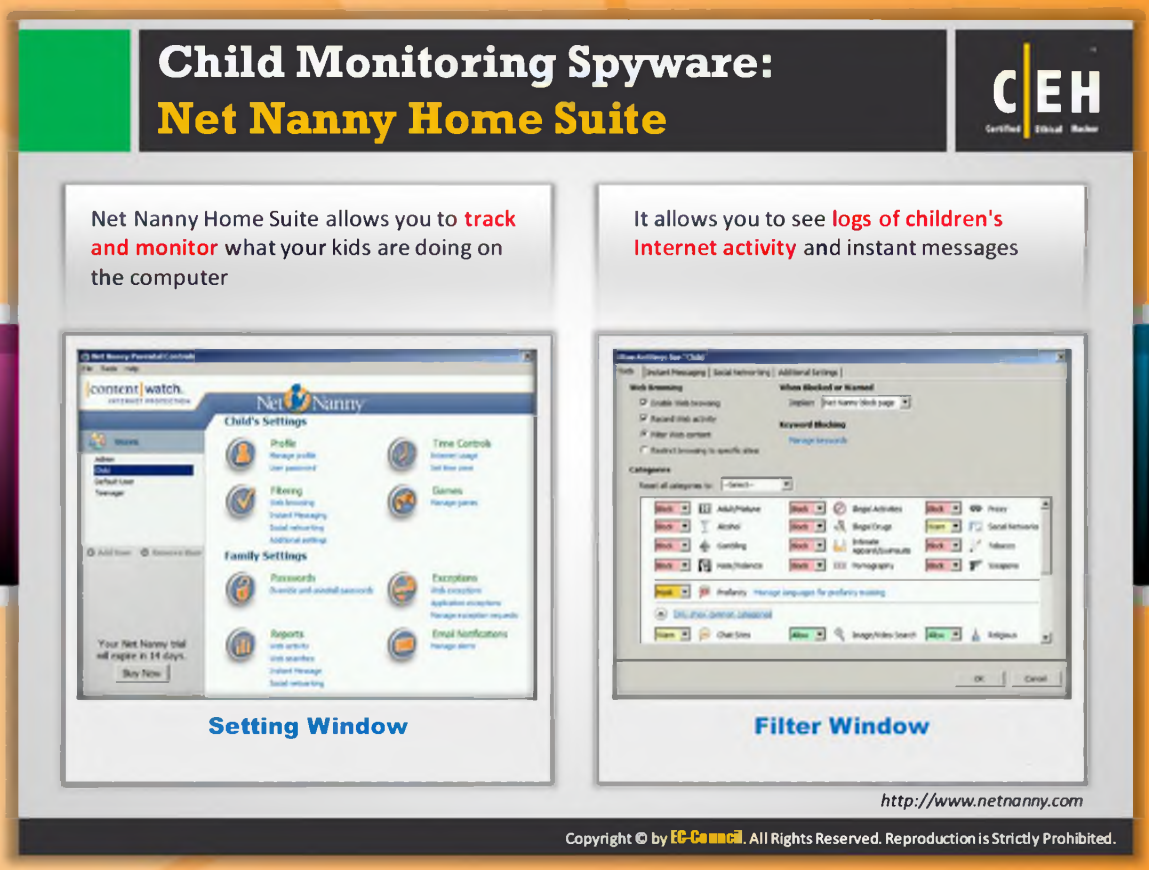


Child Monitoring Spyware

Child monitoring spyware allows you to track and monitor what your kids are doing on the computer online and offline. Instead of looking over the child's shoulder every time, one can use child monitoring spyware to know how they are spending time on the computer. This works in a stealth mode; your children will not be aware of the fact that you are watching over them. After the installation, this spyware logs the programs being used, websites visited, counts keystrokes and mouse clicks, and take screenshots of onscreen activity. All the data is accessible through a password-protected web interface.

This also allows you to protect your kids from accessing inappropriate web content by setting specific keywords that you want to block. This spyware sends a real-time alert to you whenever the specific keywords are encountered on your computer or whenever your kids want to access **inappropriate content**. It also records selected activities, including screenshots, keystrokes, and websites.

Child monitoring spyware records all the activities of your child on the computer and saves them either into a hidden encrypted file or sends to a specified email address. It also records the time at which they opened the applications, how much time they are spending on the **Internet** or **computer**, what they are doing on the computer, and so on.



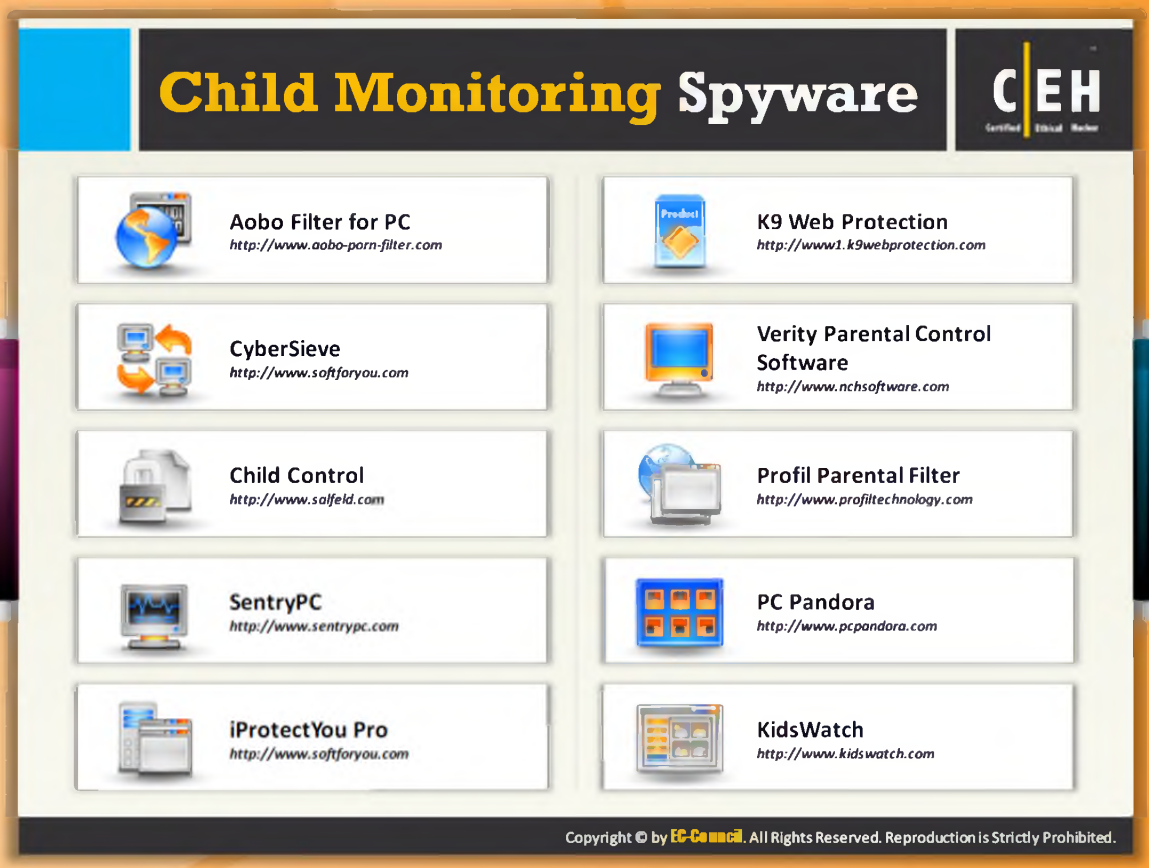
Child Monitoring Spyware: Net Nanny Home Suite

Source: http://www.netnanny.com

Net Nanny's parental control software with its Internet protection tools allows you to protect the child on the Internet from inappropriate content, pornography, and other offensive content. It is a filter that allows you to maintain your home Internet use from anywhere at any time via **remote management tools**. You can adjust the filter settings according to your personal preferences and need for monitoring web browsing and instant messaging from anywhere. It can generate alerts for IM predators and cyber bullies. It provides password-protected access for parents and customizable restrictions for each family member. You can see reports of your children's Internet activity and logs of **instant messages**.

FIGURE 5.40: Net Nanny Home Suite in Setting Window

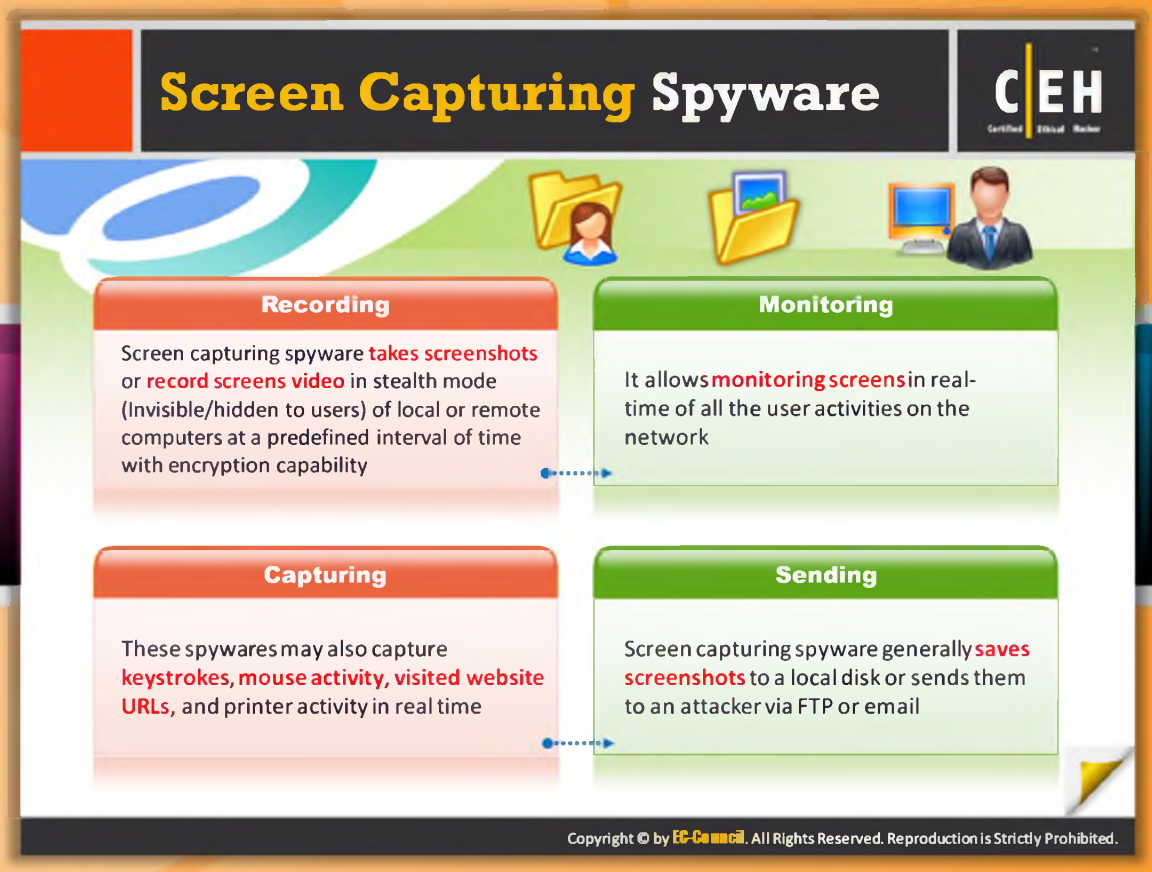
FIGURE 5.41: Net Nanny Home Suite in Filter Window



Child Monitoring Spyware

Some **child monitoring spyware** that is readily available in the market are as follows:

- Aobo Filter for PC available at http://www.aobo-porn-filter.com
- CyberSieve available at http://www.softforyou.com
- Child Control available at http://www.salfeld.com
- SentryPC available at http://www.sentrypc.com
- Spytech SentryPC available at http://www.spytech-web.com
- K9 Web Protection available at http://www1.k9webprotection.com
- Verity Parental Control Software available at http://www.nchsoftware.com
- Profil Parental Filter available at http://www.profiltechnology.com
- PC Pandora available at http://www.pcpandora.com
- KidsWatch available at http://www.kidswatch.com

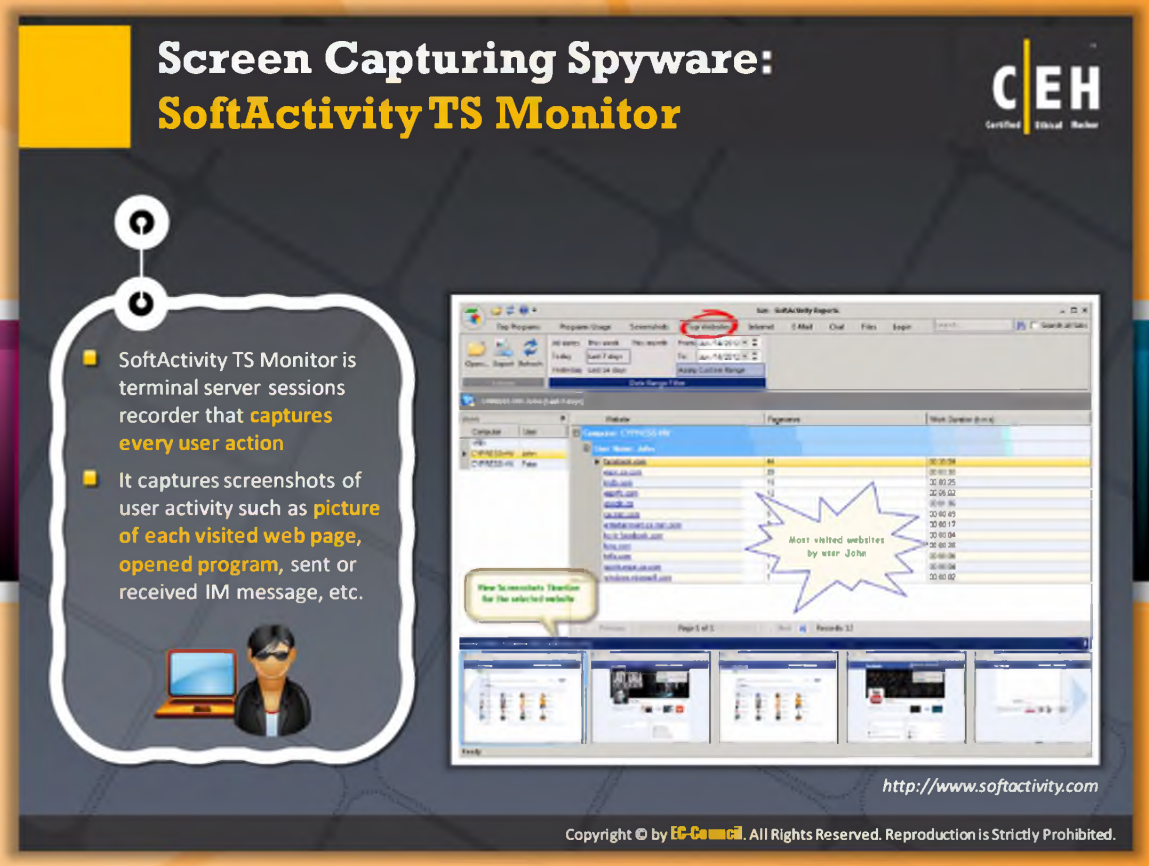


Screen Capturing Spyware

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 on the local disk in a hidden file for later review or sends them to an attacker through a predefined **email address or FTP**.

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. This program or software can be installed on networked computers to **monitor** the activities of all the computers on the network in real time by taking screen shots. This works in a **stealth mode** so you can monitor **anyone's activities** on the computer without their knowledge.

With this spyware program, users can monitor a computer and determine the activities of users on the computer as they are looking at the computer live. This program runs **transparently** in the **background**. It takes screenshots for each and every **application opened** on the computer so users can know about each and every action of the computer in real-time.



Screen Capturing Spyware: SoftActivity TS Monitor

Source: http://www.softactivity.com

SoftActivity TS Monitor is a terminal-server sessions 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**.

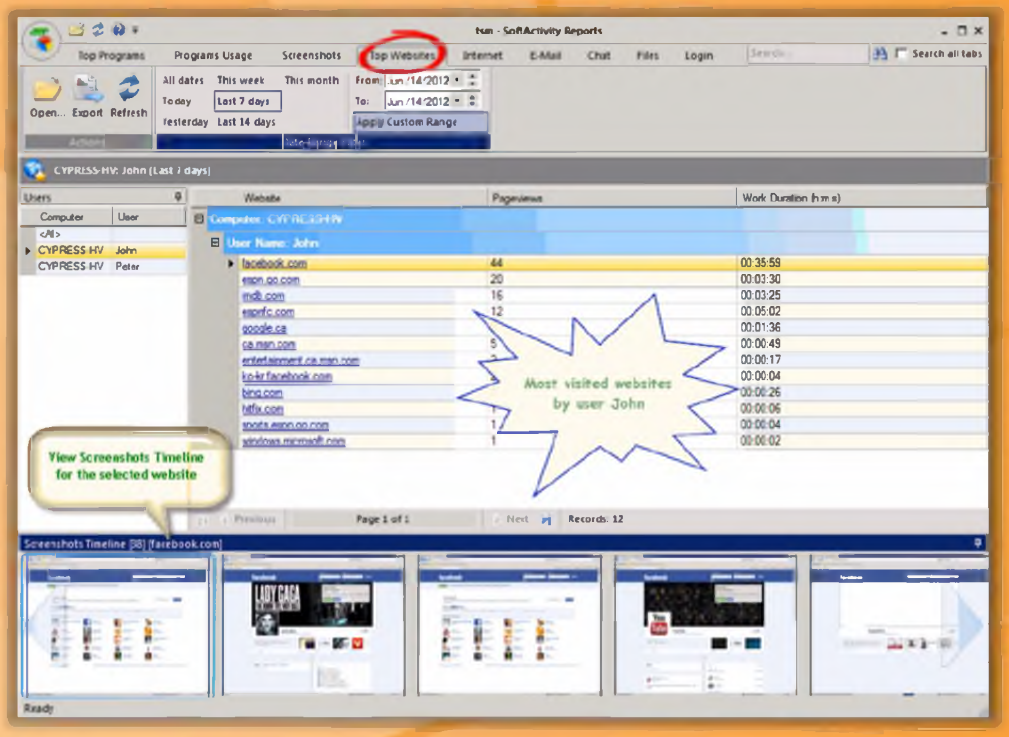
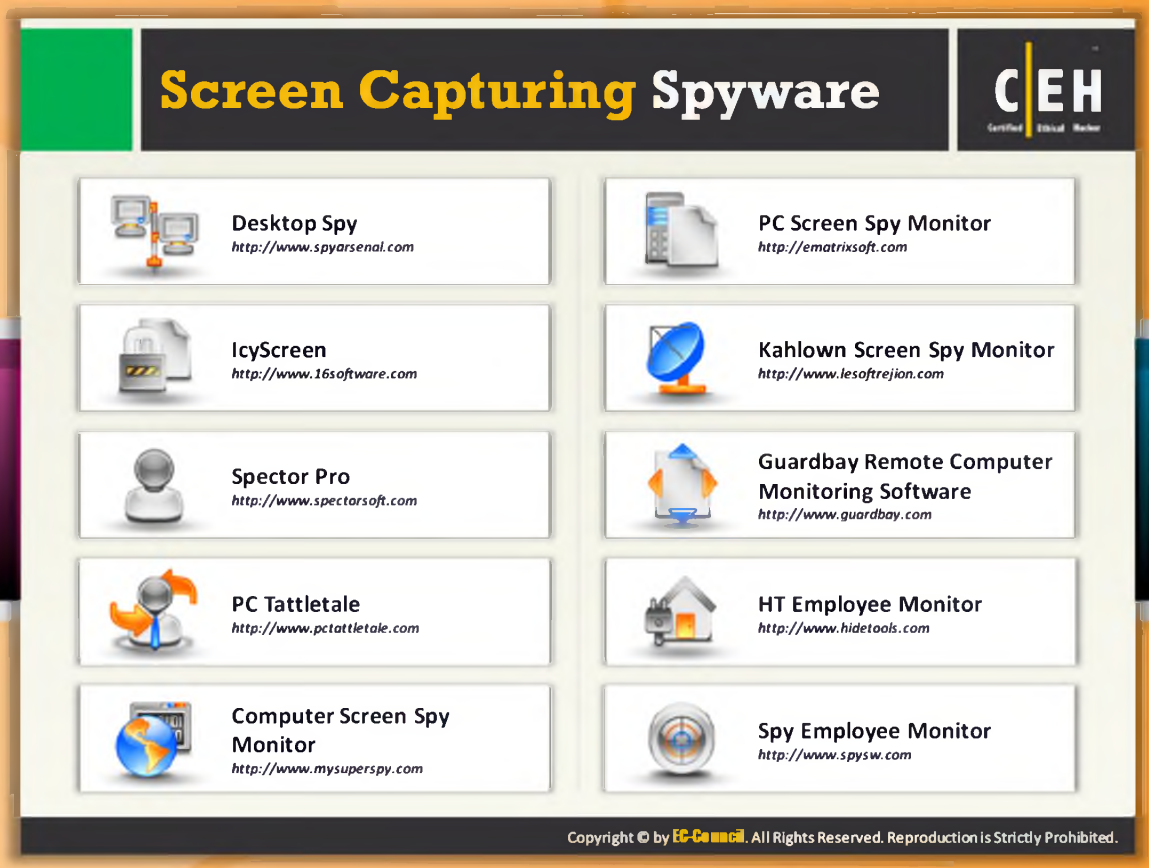


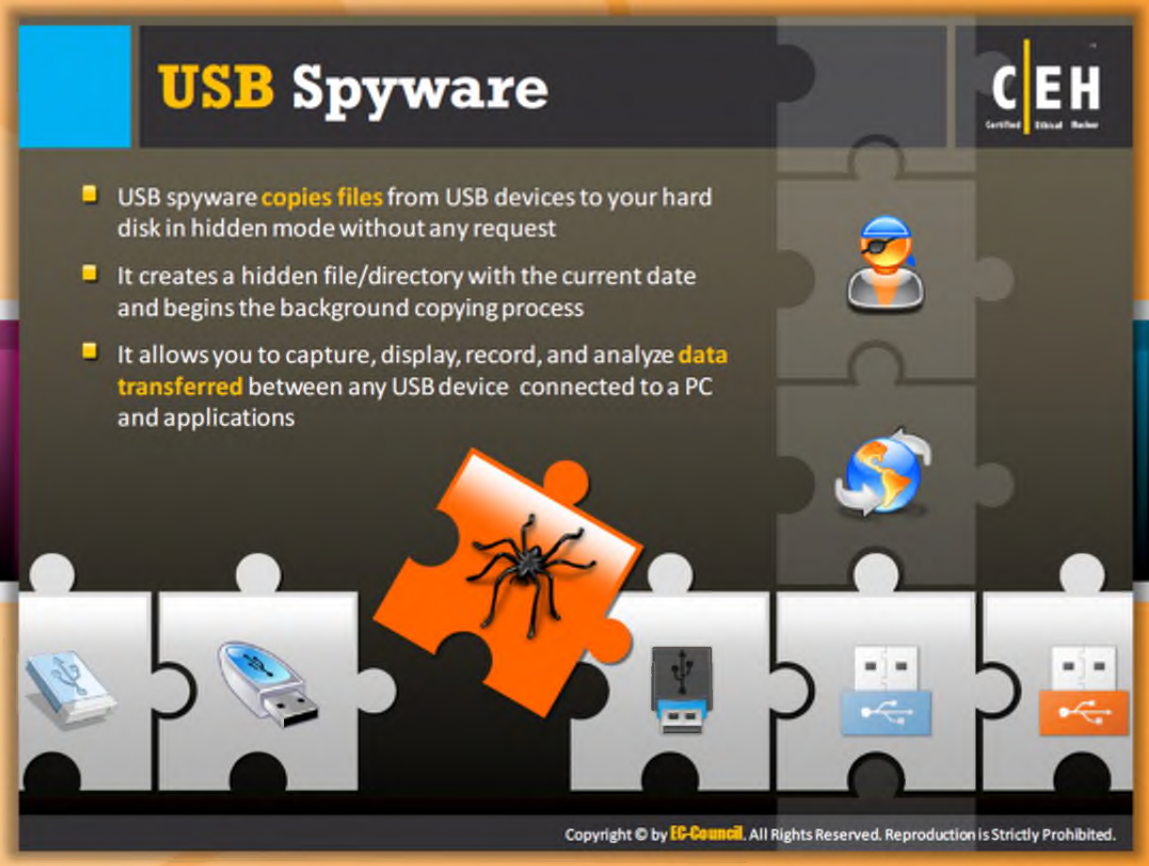
FIGURE 5.42: SoftActivity TS Monitor Screenshot



Screen Capturing Spyware

Screen capturing spyware is a program that allows you to monitor the computer **activities** of your child or employees by taking **snapshots or screenshots** for each and every application opened on the computer on which the program is installed. A few of the screen **capturing spyware** programs are listed as follows:

- Desktop Spy available at http://www.spyarsenal.com
- IcyScreen available at http://www.16software.com
- Spector Pro available at http://www.spectorsoft.com
- PC Tattletale available at http://www.pctattletale.com
- Computer Screen Spy Monitor available at http://www.mysuperspy.com
- PC Screen Spy Monitor available at http://ematrixsoft.com
- Kahlown Screen Spy Monitor available at http://www.lesoftrejion.com
- Guardbay Remote Computer Monitoring Software available at http://www.guardbay.com
- HT Employee Monitor available at http://www.hidetools.com
- Spy Employee Monitor available at http://www.spysw.com



USB Spyware

USB spyware is a program or software designed for spying on the computer and dumping into the USB device. **USB spyware** copies the spyware files from USB devices on to the hard disk without any request and notification. This **runs in a hidden mode** so the users of the computer will not be aware of the presence of the spyware on their computer.

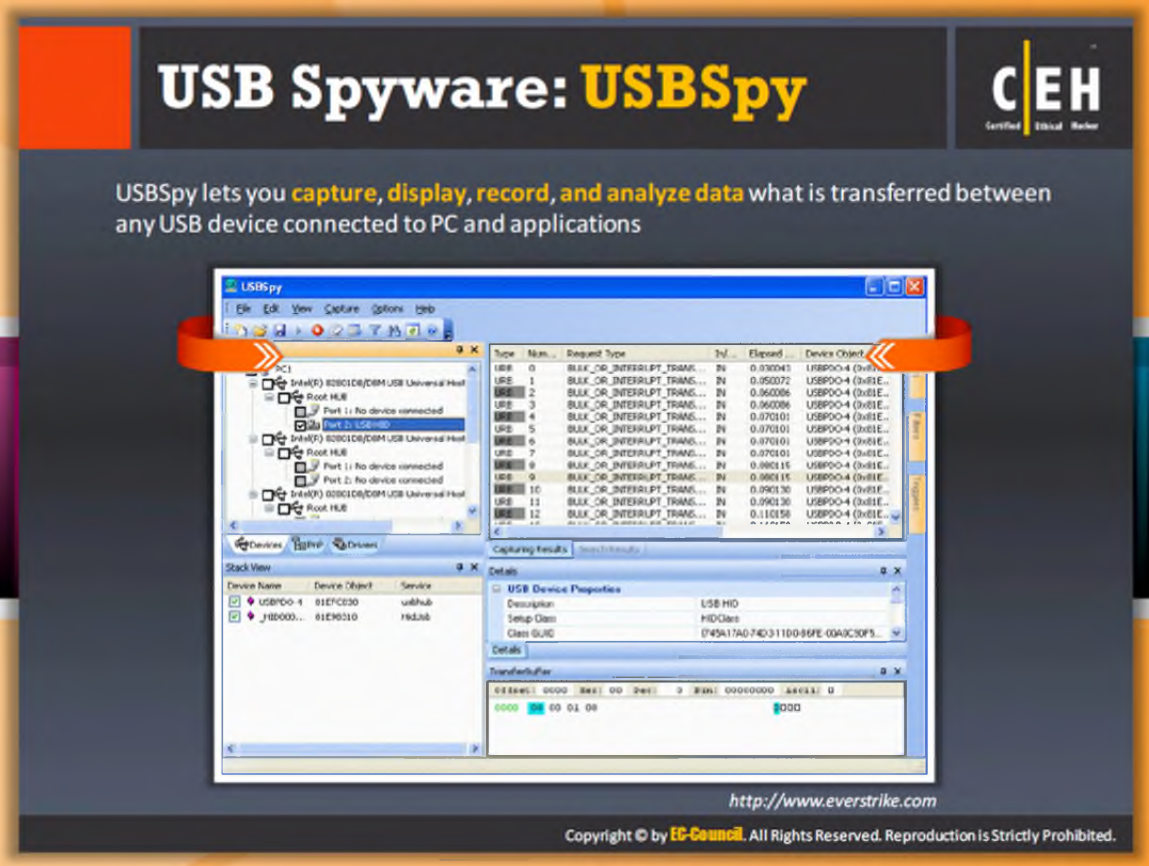
USB spyware provides a multifaceted solution in the province of USB communications. The USB spyware is capable of **monitoring USB** devices' activity without creating additional filters, devices, etc., which might damage the driver structure in the system.

USB spyware lets you capture, display, record, and analyze the data that is transferred between any USB device connected to a PC and applications. This enables working on device driver or hardware development, which provides 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 time stamp to log all the activities in the **communication sequence**.

USB spyware does not contain any **adware** or **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



USB Spyware: USBSpy

Source: http://www.everstrike.com

USBSpy lets you capture, display, record, and analyze data that is 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.

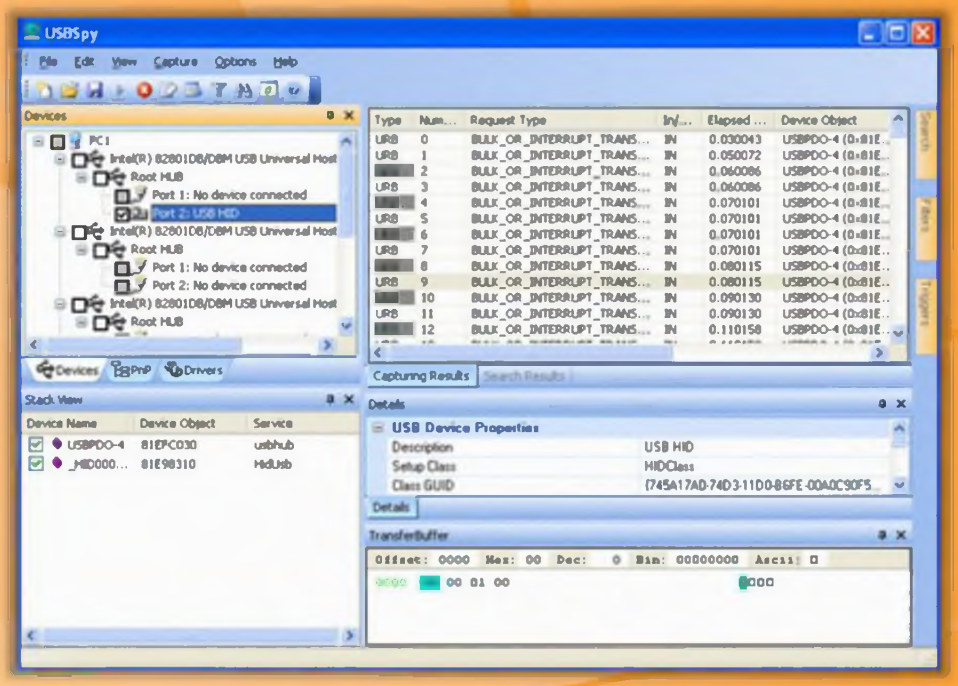


FIGURE 5.43: USB Spyware by Using USBSpy

USB Spyware

A few of **USB spyware tools** that are available in the market are listed as follows:

- USB Monitor available at http://www.hhdsoftware.com
- USB Grabber available at http://usbgrabber.sourceforge.net
- USBTrace available at http://www.sysnucleus.com
- USBDeview available at http://www.nirsoft.net
- Advanced USB Port Monitor available at http://www.aggsoft.com
- USB Monitor Pro available at http://www.usb-monitor.com
- USB Activity Monitoring Software available at http://www.datadoctor.org
- Stealth iBot Computer Spy available at http://www.brickhousesecurity.com
- KeyCarbon USB Hardware Keylogger available at http://www.spywaredirect.net
- USB 2GB Keylogger available at http://diij.com

Audio Spyware

Audio spyware is the **sound surveillance program** that is designed to capture the sound waves or voice onto the computer. The spyware can be installed on the computer without the permission of the computer user. The audio spyware is installed on the computer in a silent manner without **sending any notification** to the user and runs in the background to record various sounds on the computer secretly. Using **audio spyware** doesn't require any **administrative privileges**.

Audio spyware monitors and records a variety of sounds on the computer. The recorded sounds are saved into a hidden file on the local disk for later retrieve. Therefore, attackers or malicious users use this audio spyware to snoop and **monitor conference recordings**, phone calls, and radio broadcasts, which may contain the confidential information.

Audio spyware 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 who they are **communicating** with.

Audio spyware can be used 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, etc. They allow live call monitoring, audio **surveillance**, track SMS, logging all calls, and GPRS tracking.

Audio Spyware: Spy Voice Recorder and Sound Snooper

Spy Voice Recorder

Source: http://www.mysuperspy.com

Spy Voice Recorder is 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, etc.

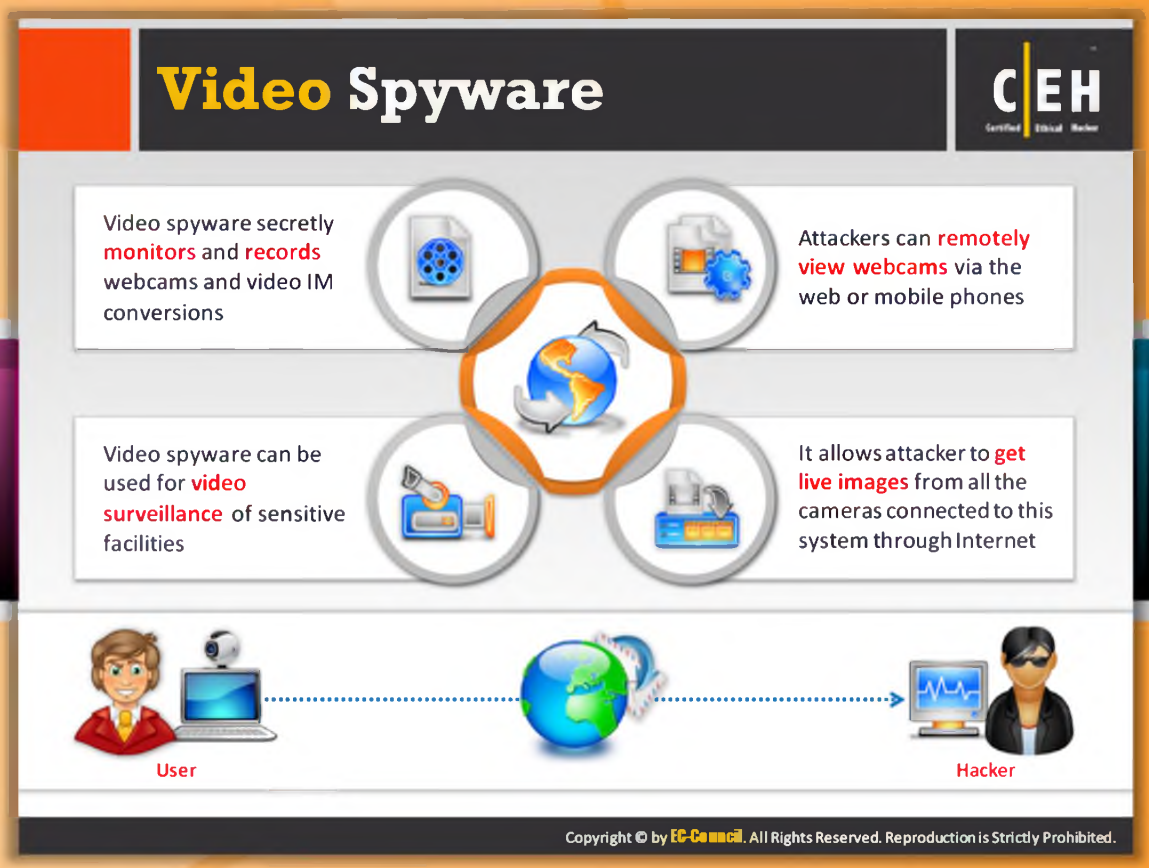
FIGURE 5.44: Spy Voice Recorder Screenshot

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**, etc. 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**.

FIGURE 5.45: Sound Snooper Screenshot



Video Spyware

Video spyware is software for video surveillance. With this software, you can record all video activity with a programmed schedule. This can be installed on the **target** computer without the user's knowledge. The video spyware runs transparently in the background, and monitors and records webcams and **video IM conversions** secretly. The remote access feature of video spyware allows the attacker to connect to the remote or target system in order 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.

Video Spyware: WebCam Recorder

Source: http://webcamrecorder.com

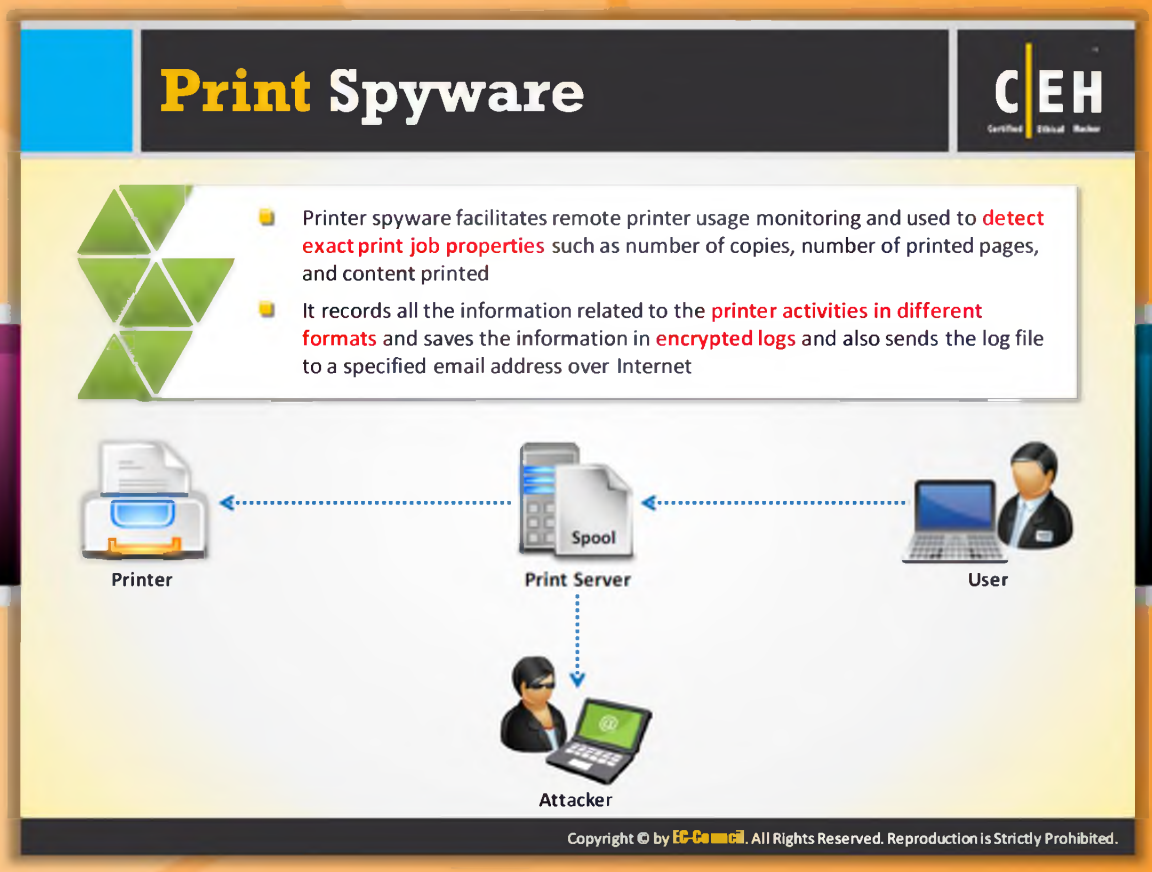
WebCam Recorder is video surveillance software that allows you to record anything on screen such as webcams playing in your browser, video IM conversations, content from video sites such as YouTube, and video playing on your **desktop**.

FIGURE 5.46: Video Spyware by Using WebCam Recorder

Video Spyware

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

- WebcamMagic available at http://www.robomagic.com
- MyWebcam Broadcaster available at http://www.eyespyfx.com
- I-Can-See-You available at http://www.internetsafetysoftware.com
- Digi-Watcher available at http://www.digi-watcher.com
- NET Video Spy available at http://www.sarbash.com
- Eyeline Video Surveillance Software available at http://www.nchsoftware.com
- Capturix VideoSpy available at http://www.capturix.com
- WebCam Looker available at http://felenasoft.com
- SecuritySpy available at http://www.bensoftware.com
- iSpy available at http://www.ispyconnect.com



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, etc. It records all information related to the printer activities and saves the information in **encrypted logs** 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 web format for sending the reports to an email through the web or **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 were printed by each employee or workstation, 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** that have been printed.

FIGURE 5.47: Working of Print Spyware

Print Spyware: Printer Activity Monitor

Source: http://www.redline-software.com

Printer Activity Monitor is one of the **print spyware programs** that an attacker can use to monitor printer usage of the target organization to get information about printed documents. This spyware allows attackers to **monitor** and **audit printers** so that he or she can find out which documents are printed on each of the selected printers, the number of pages printed, etc.

Attackers can do the following things with help of Printer Activity Monitor:

- Accurately track print jobs
- Monitor large numbers of printers simultaneously
- **Monitor** printers remotely
- Generate **reports** about printer usage

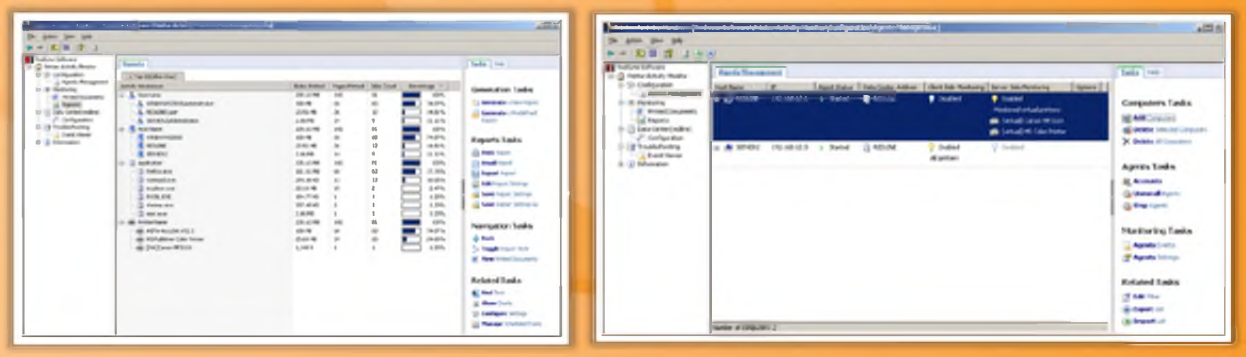


FIGURE 5.48: Print Spywareby Using Printer Activity Monito

Print Spyware

Attackers can also use the following printer monitoring applications as **printer spyware** to get information about target printer usage. This printer spyware helps attackers to **track printer usage** such as content of documents printed, number copies printed, date and time at which the print action took place, and so on. A few print spyware programs are listed as follows:

- Print Monitor Pro available at http://www.spyarsenal.com
- Accurate Printer Monitor available at http://www.aggsoft.com
- Print Censor Professional available at http://usefulsoft.com
- All-Spy Print available at http://www.all-spy.com
- O&K Print Watch available at http://www.prnwatch.com
- Print Job Monitor available at http://www.imonitorsoft.com
- PrintTrak available at http://www.lygil.com
- Printer Admin - Copier Tracking System available at http://www.printeradmin.com
- Print Inspector available at http://www.softperfect.com
- Print365 available at http://krawasoft.com

Telephone/Cell Phone 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 can be used 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/cell phone spyware features include:

- **Call History** - allows you to see the entire call history of the phone (both incoming & outgoing calls).
- **View Text Messages** – enables you to view all **incoming** and **outgoing text messages**. Even deleted messages can be viewed in the log report.
- **Web Site History** – the entire history of all websites visited through the phone will be recorded to the log report file.

- **GPS Tracking** – The spyware will show 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.

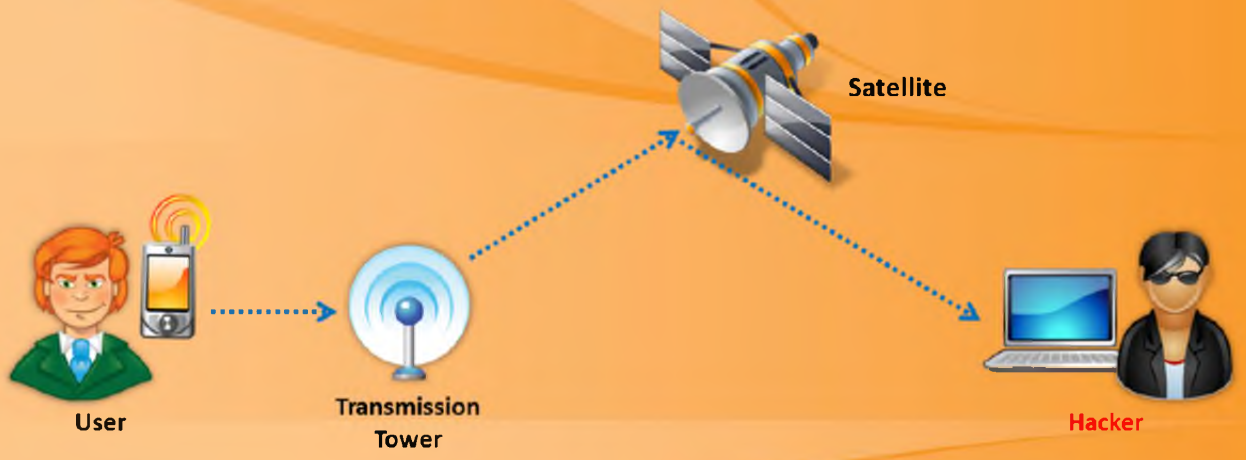


FIGURE 5.49: Working of Telephone/Cell Phone Spyware

Cellphone Spyware: Mobile Spy

Source: http://www.phonespysoftware.com

Mobile Spy is mobile spyware that helps you to monitor and record the activities of a **target mobile phone**. You need to install this software on the mobile phone. With help of this software, you can record activities, logs, and **GPS locations** of target. To view the results, you simply need to log in to your **secure account** using any computer or mobile web browser. Logs are displayed by **categories** and sorted 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 details, etc.

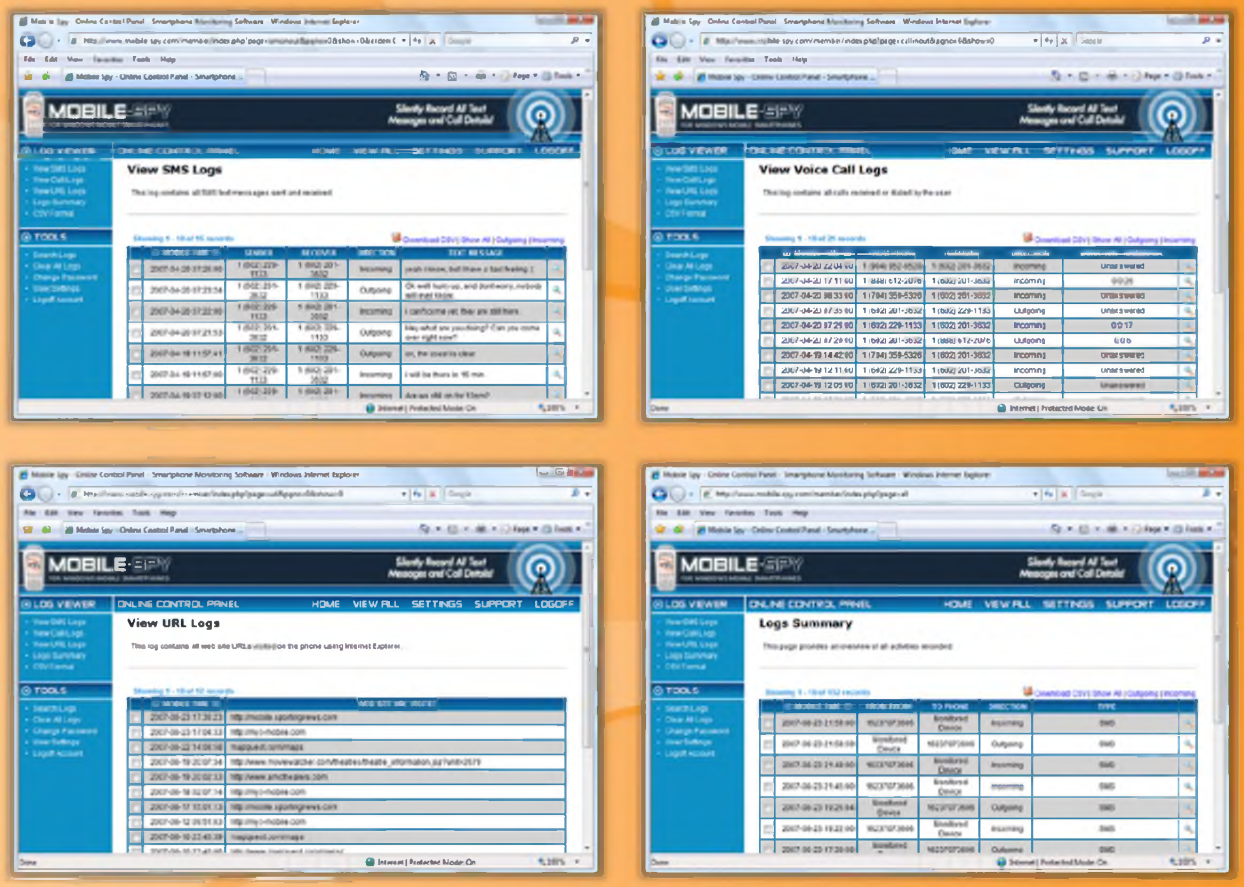
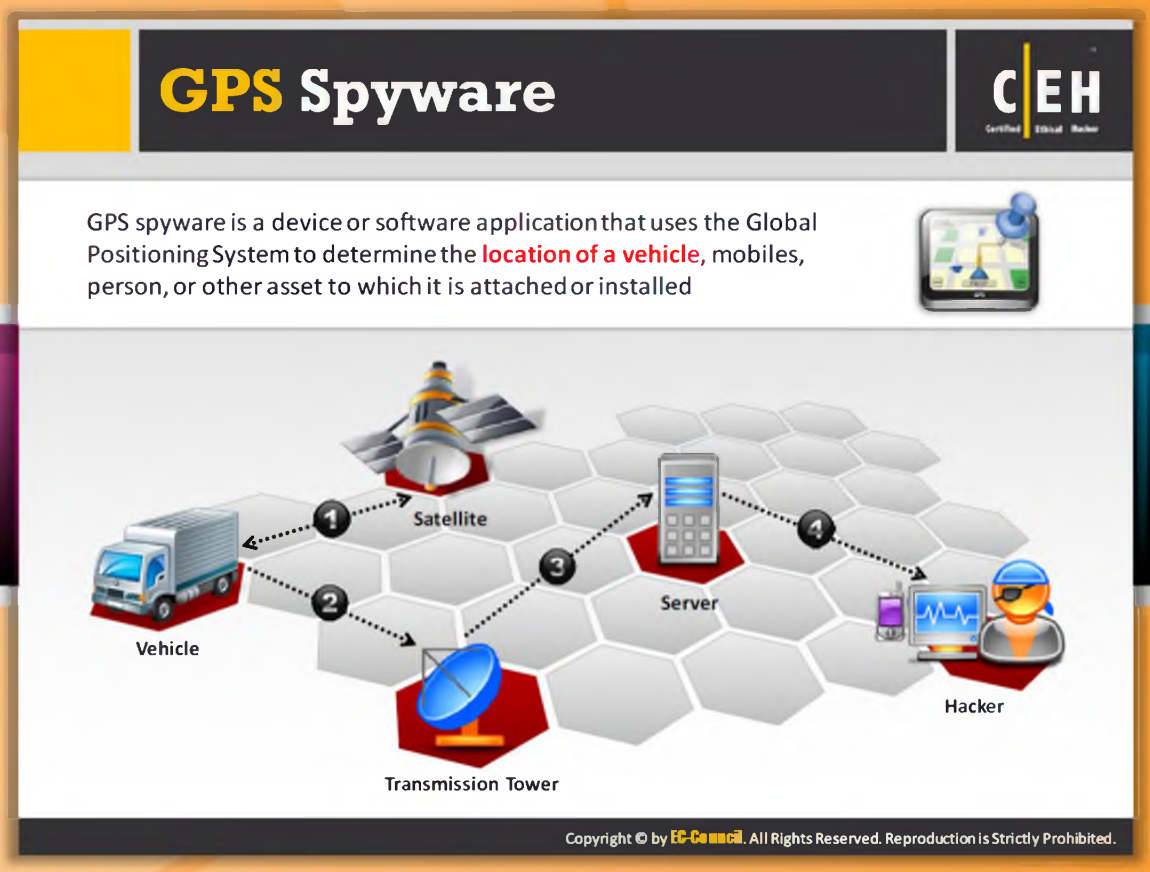


FIGURE 5.50: Cellphone Spyware by Using Mobile Spy

Telephone/Cell Phone Spyware

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

- VRS Recording System available at http://www.nch.com.au
- Modem Spy available at http://www.modemspy.com
- MobiStealth Cell Phone Spy available at http://www.mobistealth.com
- SPYPhone GOLD available at http://spyera.com
- SpyPhoneTap available at http://www.spyphonetap.com
- FlexiSPY OMNI available at http://www.flexispy.com
- SpyBubble available at http://www.spybubble.com
- MOBILE SPY available at http://www.mobile-spy.com
- StealthGenie available at http://www.stealthgenie.com
- CellSPYExpert available at http://www.cellspyexpert.com/



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 asset to which it is attached or installed. 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. This 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.

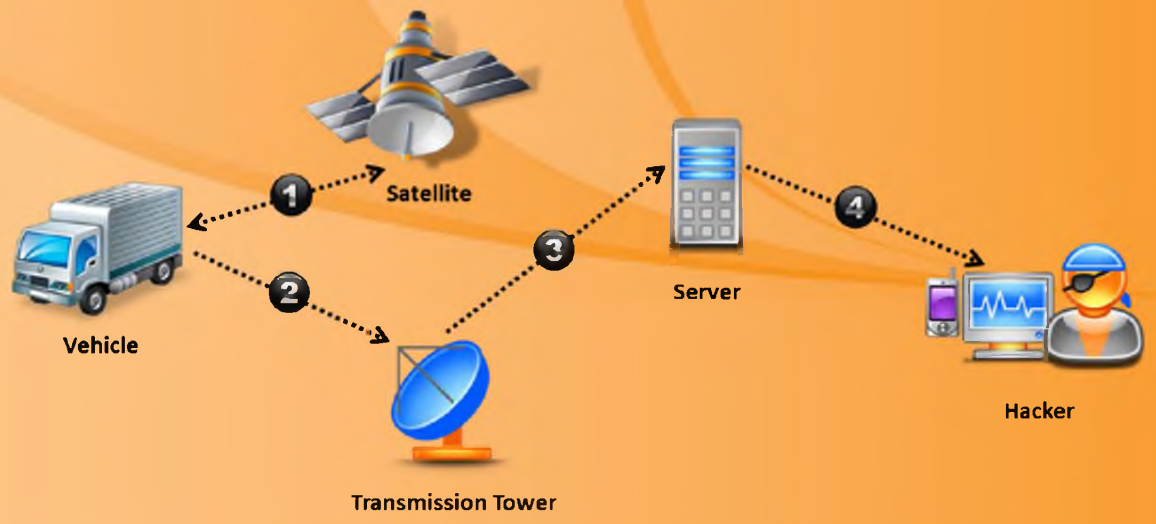
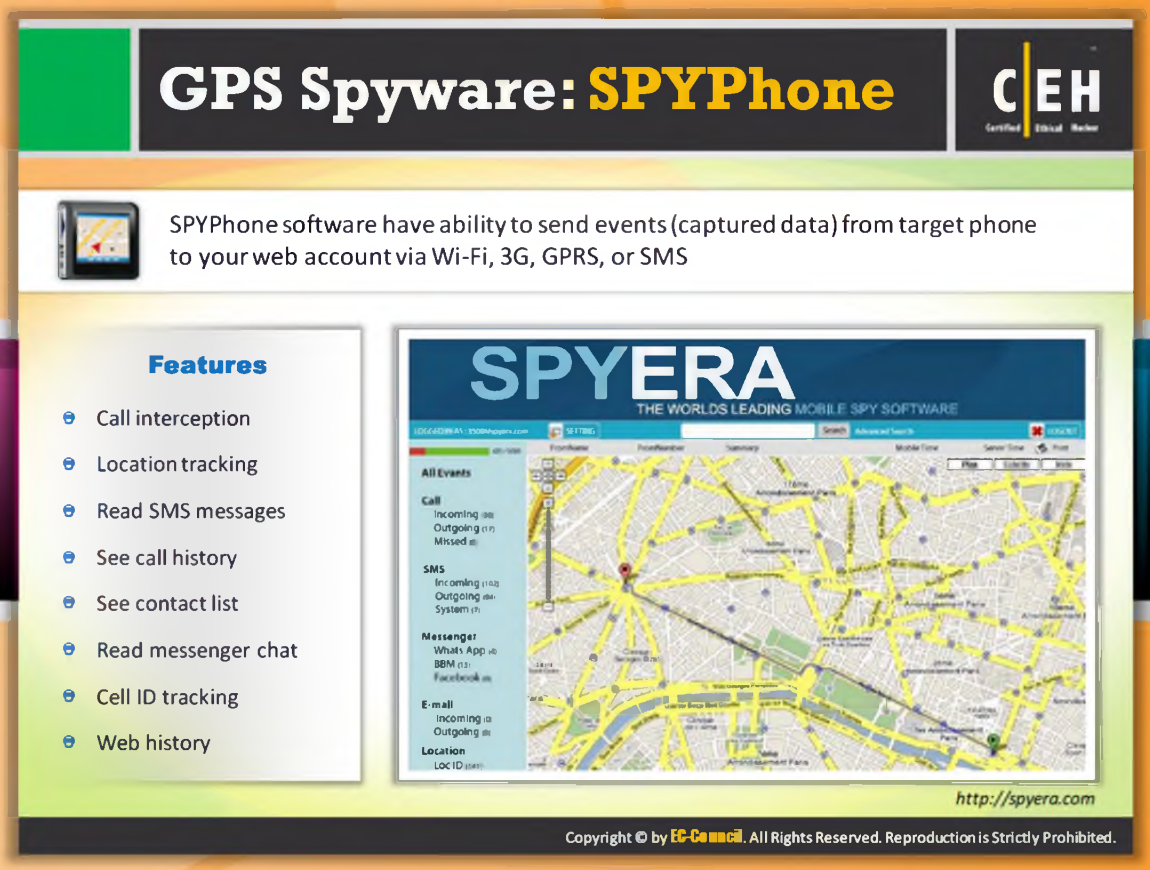


FIGURE 5.51: Working of GPS Spyware



GPS Spyware: SPYPhone

Source: http://spyera.com

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

FIGURE 5.52: GPS Spyware of Using SPYPhone

GPS Spyware

There are **various software programs** that can be used 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 available at http://www.easygps.com
- FlexiSPY PRO-X available at http://www.flexispy.com
- GPS TrackMaker Professional available at http://www.gpstm.com
- MOBILE SPY available at http://www.mobile-spy.com
- World-Tracker available at http://www.world-tracker.com
- ALL-in-ONE Spy available at http://www.thespyphone.com
- Trackstick available at http://www.trackstick.com
- MobiStealth Pro available at http://www.mobistealth.com
- mSpy available at http://www.buymspy.com
- GPS Retriever available at http://www.mobilebugstore.com

How to Defend Against Keyloggers

A keylogger is a **software application** that **secretly captures** and **records** all keystrokes including passwords that are typed on the computer keyboard. The main objective behind developing keylogger software was for positive productive usage such as recovering lost or deleted data, monitoring employees or children, and diagnosing other computer system problems. However, attackers used keyloggers for malicious purposes such as identity theft of employees, cracking passwords, acquiring credit card and bank account numbers and phone numbers, **gaining unauthorized access**, and so on. Though it is difficult to detect the presence of **keyloggers** as they are hidden on the system, here are a few ways to defend against keyloggers:

- **Install antivirus** and antispyware software. Viruses, Trojans, and other malware are the mediums through which software keyloggers invade the computer. Antivirus and **antispyware** are the first line of defense against keyloggers. Using keylogger cleaning applications available online, keyloggers detected by the antivirus can be deleted from the computer.
- Install host-based IDS, which can monitor your system and **disable** the **installation** of keyloggers.

- Enable firewalls on the computer. Firewalls prevent outside access to the computer. **Firewalls prevent** the **transmission** of recorded information back to the attacker.
- Keep track of the programs that are running on the computer. Use software that frequently scans and monitors the changes in the system or network. Usually keyloggers tend to run in the **background transparently**.
- 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**.
- Recognize and delete phishing emails because most attackers use **phishing emails** as a medium to transfer software keyloggers to a victim's system.

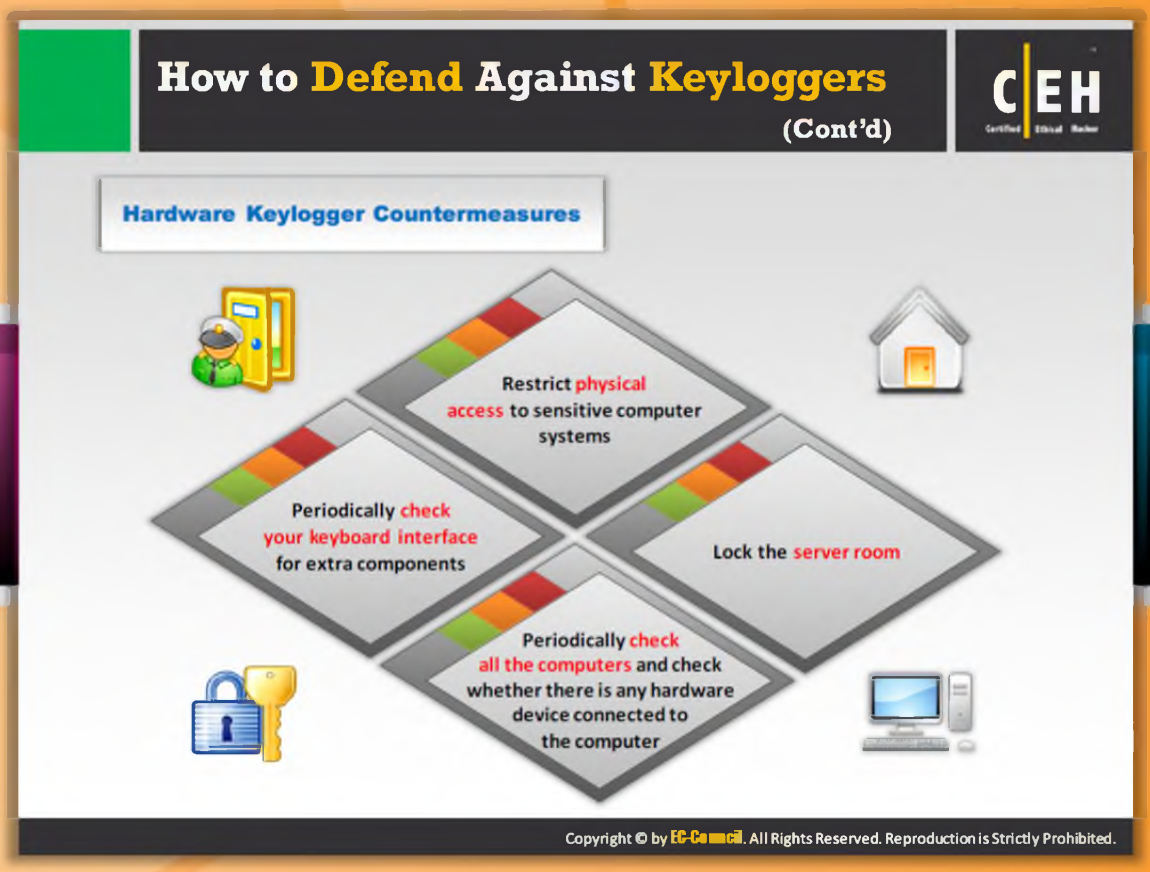
How to Defend Against Keyloggers (Cont'd)

The following are some more ways to defend against keyloggers:

- Enable **pop-up blockers** and avoid opening junk emails and their attachments.
- Antivirus and antispyware software is able to detect anything that gets installed, but it is better to detect these programs before they are installed. Scan the files thoroughly before installing them on to the computer and use a **registry editor** or process explorer to check for keystroke loggers.
- Use live **CD/DVD** or write-protected Live USB to reboot the computer.
- 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 here the mouse is used for entering any information such as passwords, credit

card numbers, etc. into the keyboard instead of typing the passwords using the keyboard.

- Do not click on links in unwanted or **suspicious emails** that may point you to malicious websites.



How to Defend Against Keyloggers (Cont'd)

The countermeasures mentioned so far provide protection against software keyloggers. Now we will discuss hardware keyloggers. A hardware keylogger is a hardware device that records each and every keystroke that is typed on the computer keyboard in real time. This device is plugged in between the computer case and keyboard cable connector. A keylogger is used for legitimate applications as well as by attackers for deceitful purposes such as for stealing passwords, bank account numbers, phone numbers and so on. To defend your system against keyloggers, follow the countermeasures listed as follows:

- Restrict physical access to sensitive computer systems
- Periodically check your keyboard interface to ensure that no extra components are plugged to the keyboard cable connector
- Lock the server room
- Periodically check all the computers and check whether there is any hardware device connected to them

Anti-Keyloggers

Anti-keyloggers, also called anti-keystroke loggers, are designed especially for detecting and **disabling keystroke logger software**. Anti-keyloggers are specially designed for the purpose of detecting 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 that is 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.

FIGURE 5.53: Anti-Keylogger Screenshot

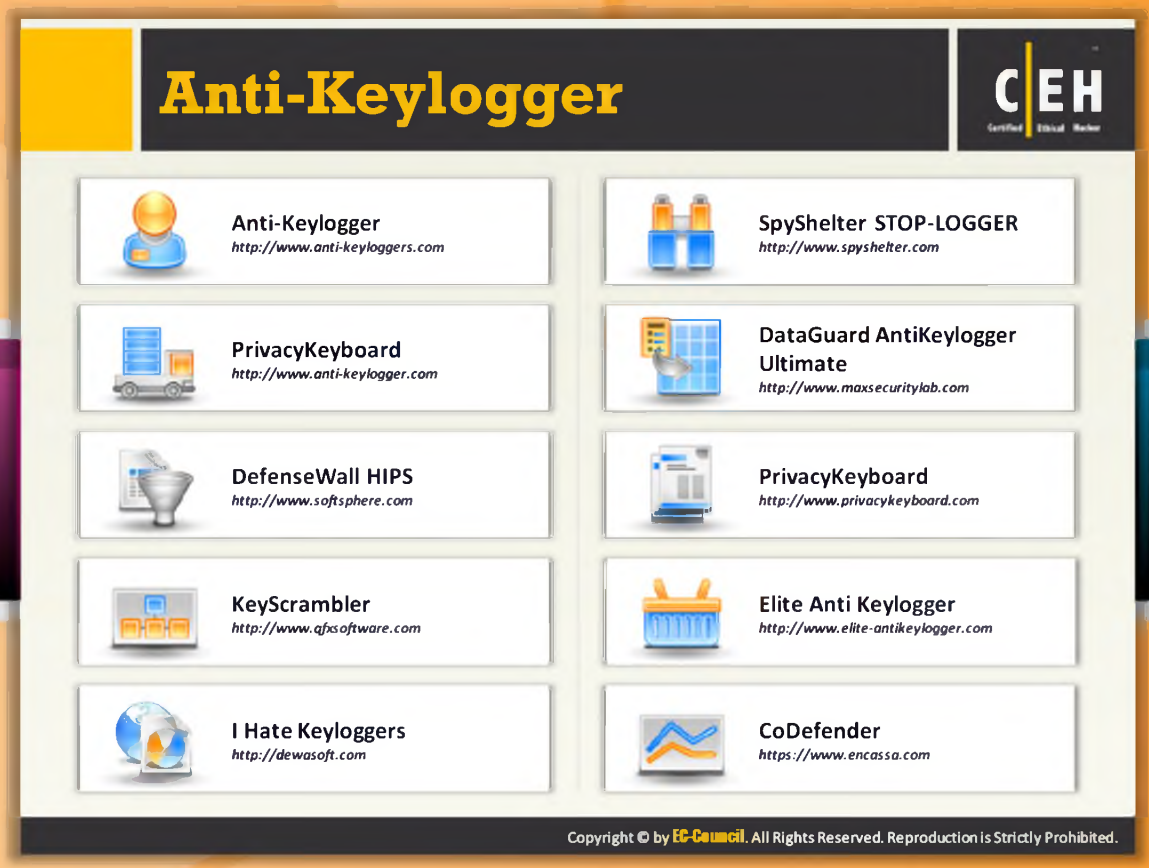
Anti-Keylogger: Zemana AntiLogger

Source: http://www.zemana.com

Zemana Antilogger is a high-performance security program that 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 Antilogger provides protection against various threats such as SSL logger, Webcam logger, Keyloggers, Clipboard logger, Screen logger, spyware, SSL banker, Trojans, etc.

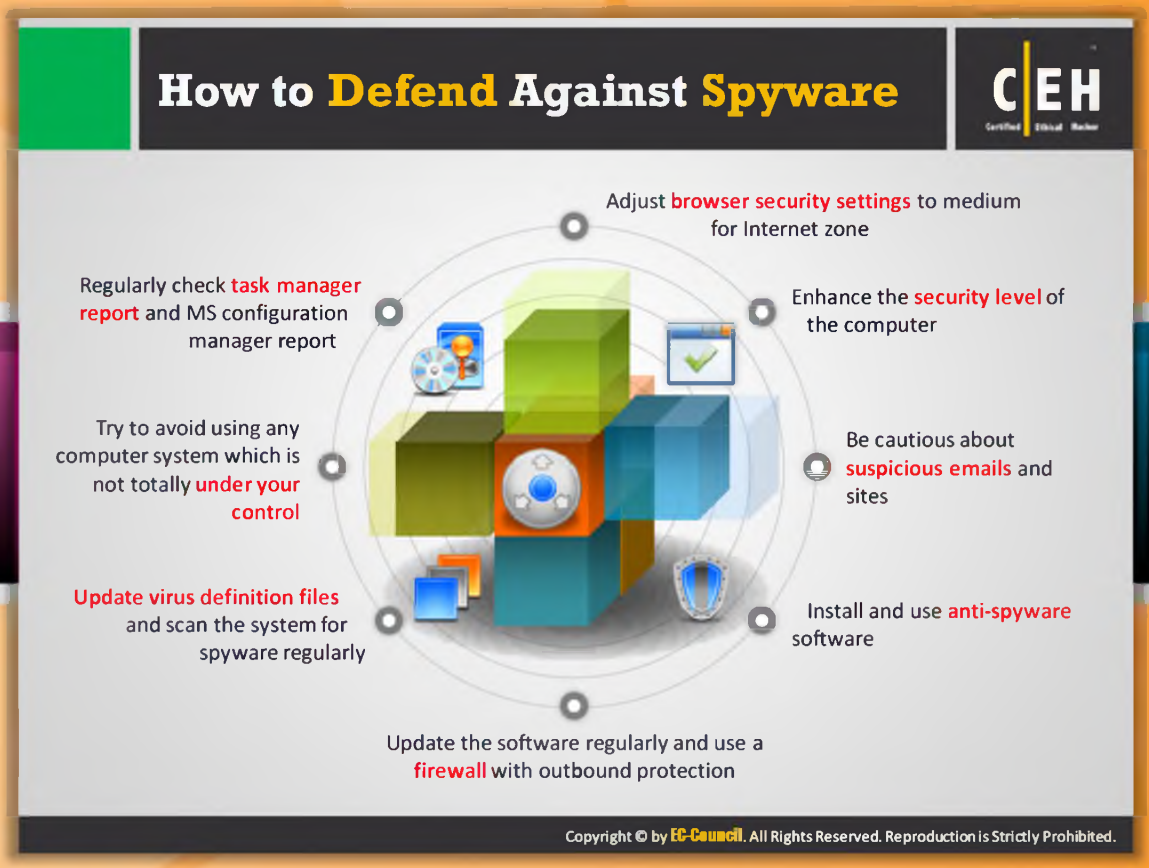
FIGURE 5.54: Zemana AntiLogger Screenshot



Anti-Keyloggers

Anti-keyloggers secure your system from spyware attacks, software keyloggers, and hardware keyloggers. Some of **anti-keyloggers** that can be used for securing your system against various threats are listed as follows:

- Anti-Keylogger available at http://www.anti-keyloggers.com
- PrivacyKeyboard available at http://www.anti-keylogger.com
- DefenseWall HIPS available at http://www.softsphere.com
- KeyScrambler available at http://www.qfxsoftware.com
- I Hate Keyloggers available at http://dewasoft.com
- SpyShelter STOP-LOGGER available at http://www.spyshelter.com
- DataGuard AntiKeylogger Ultimate available at http://www.maxsecuritylab.com
- PrivacyKeyboard available at http://www.privacykeyboard.com
- Elite Anti Keylogger available at http://www.elite-antikeylogger.com
- CoDefender available at https://www.encassa.com



How to Defend Against Spyware

Spyware is a malicious program that gets installed onto a user system without the user's knowledge and gathers confidential information such as personal data, access logs, etc. Spyware comes from **three basic sources**: one of the main sources is through free downloaded software, the second source of spyware is through email attachments, and the third source of spyware is websites that automatically install spyware when you. Here are ways to defend against spyware:

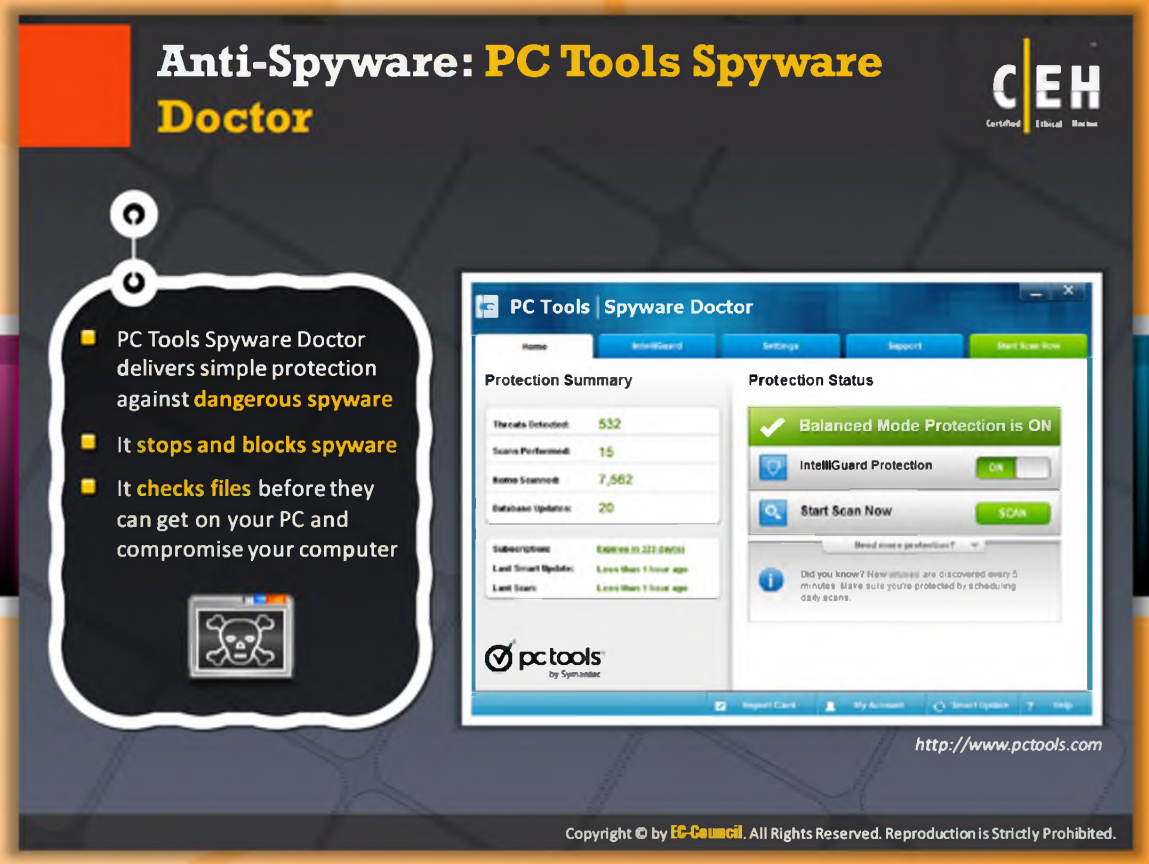
- Never adjust your Internet **security setting** level too low because it provides many chances for spyware to be installed on your computer. So, always set your Internet browser security setting to either high or medium for **protecting** your computer from spyware.
- Firewall enhances the security 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 that are presented in spam mail messages, **retrieved** by search engines, or displayed in **pop-up windows** because they may mislead you to download spyware.

- Install antispyware software. **Antispyware** protects against spyware. Antispyware is the first line of defense against spyware. This software prevents spyware from being installed on your system. It periodically scans your system and protects your system from spyware.
- Regularly check Task Manager reports and MS **Configuration** Manager reports.
- Try to avoid using any computer system that is not totally under your control.
- **Update** virus definition files and scan the system for spyware on a regular basis.

How to Defend Against Spyware (Cont'd)

- Always use caution with anything found on the Internet while **downloading** and **installing free software**. Before downloading any software, make sure that it is from a trusted website. The license agreement, security warning, and **privacy statements** that are associated with the software should be read thoroughly to get a clear understanding before you download.
- Do not use **administrative mode** unless it is necessary because malicious programs such as spyware are executed when you are 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 they are accessed by many users. 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.
- Permanently **delete cookies**, caches, URLs, history and **temporary files** on the computer when done web surfing.
- Do not store personal or financial information on any computer system that is not totally under your control, such as in an **Internet café**.

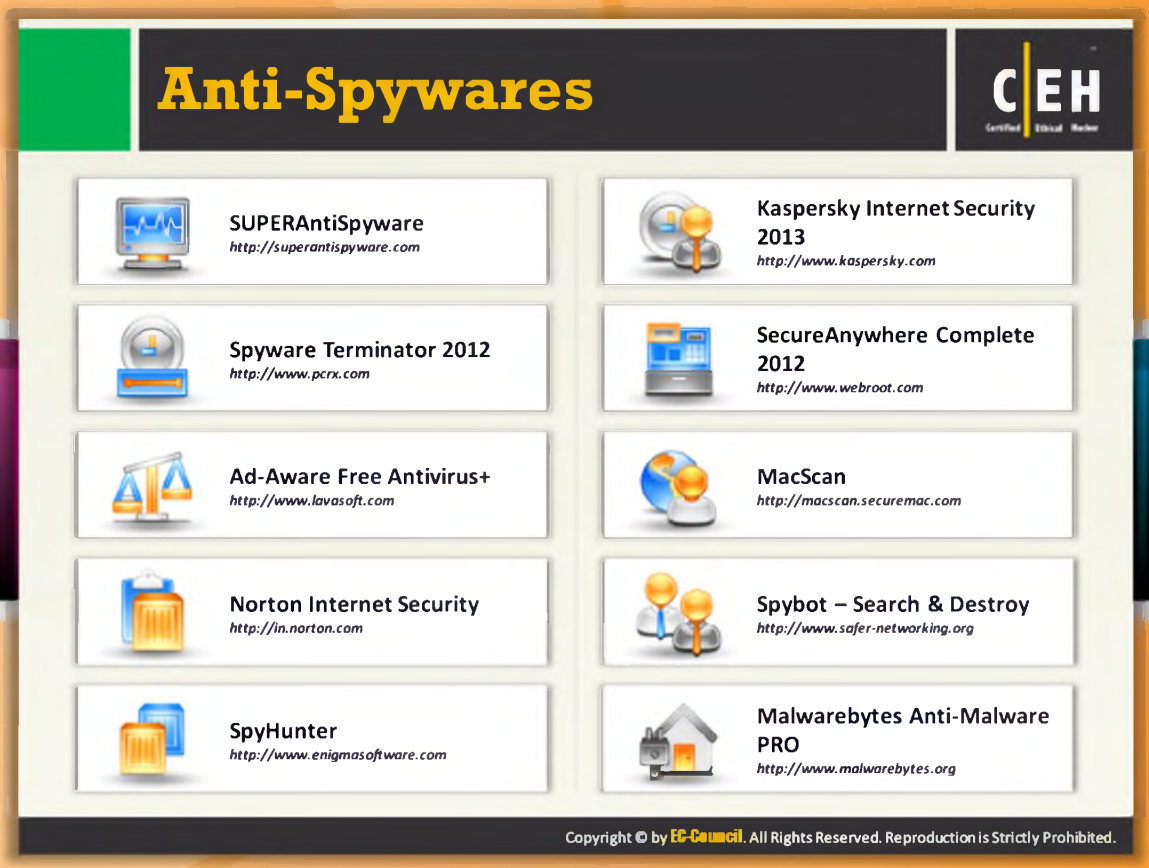


Anti-Spyware: PC Tools Spyware Doctor

Source: http://www.pctools.com

PC Tools Spyware Doctor provides protection for your system against extremely dangerous spyware and malware. It detects and deactivates various **malicious programs** such as adware, trojans, keyloggers, spybots, etc. from your system. It is quite easy to protect your **confidential** or financial information against spyware using this. Even dangerous threats can be easily defended when this software is **integrated** with various layers of protection. The files are checked thoroughly before spyware actually enters and **compromises** your system.

FIGURE 5.55: PC Tools Spyware Doctor Screenshot



Anti -Spywares

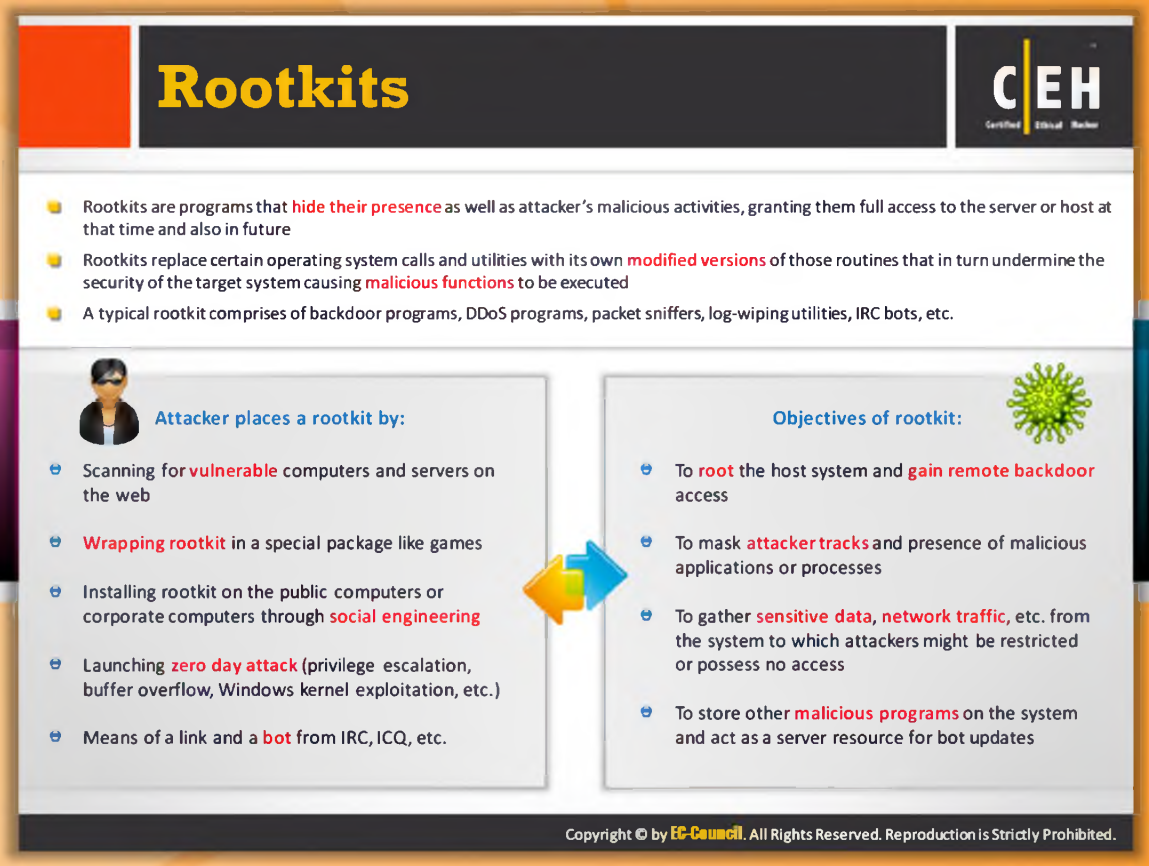
Antispywares scan your system and check for spyware such as malware, Trojans, dialers, worms, keyloggers, and rootkits and removes them if any are found. Antispyware provides **real-time protection** by scanning your system at regular intervals, either weekly or daily. It scans to ensure the computer is free from **malicious software**. A few antispyware programs are listed as follows:

- SUPERAntiSpyware available at http://superantispyware.com
- Spyware Terminator 2012 available at http://www.pcrx.com
- Ad-Aware Free Antivirus+ available at http://www.lavasoft.com
- Norton Internet Security available at http://in.norton.com
- SpyHunter available at http://www.enigmasoftware.com
- Kaspersky Internet Security 2013 available at http://www.kaspersky.com
- SecureAnywhere Complete 2012 available at http://www.webroot.com
- MacScan available at http://macscan.securemac.com
- Spybot – Search & Destroy available at http://www.safer-networking.org
- Malwarebytes Anti-Malware PRO available at http://www.malwarebytes.org

CEH System Hacking Steps

Like **malicious applications**, there are also many **protective applications** that are capable of preventing or detecting and deleting malicious applications. In order to avoid malicious applications being detected by **protective applications**, attackers hide malicious files inside other **legitimate files**.

Cracking Passwords	Hiding Files
Escalating Privileges	Covering Tracks
Executing Applications	Penetration Testing



Rootkits

Rootkits are software programs aimed to gain access to a computer without being detected. These are malware that can be used 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, etc. It works by exploiting the vulnerabilities in the operating system and applications. It builds a **backdoor login process** to the operating system by which the attacker can evade the standard login process. Once root access has been enabled, a rootkit may attempt to hide the traces of **unauthorized access** by **modifying drivers** or **kernel modules** and deserting 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 causing **malicious functions** to be executed. A typical **rootkit** is **comprised** of backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.

All files contain a set of attributes. There are different fields in the file attributes. The first field is used to determine the format of the file, that is, if it is a hidden, archive, or read-only file. The other field describes the time the file was created, when it was accessed, as well as its original length. The functions GetFileAttributesEx() and GetFileInformationByHandle() enable this. ATTRIB.exe is used to display or change file attributes. An attacker can hide, or even change the attributes of a victim's files, so that attacker can access them.

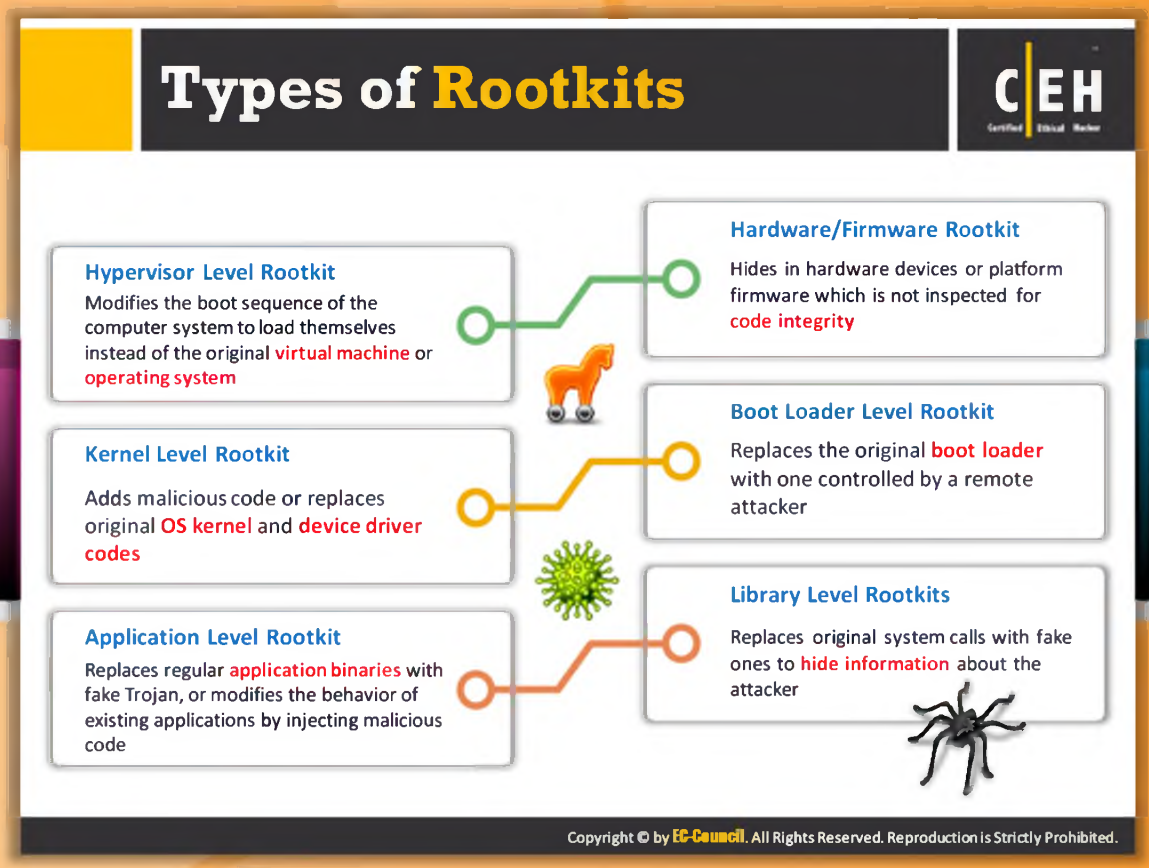
An attacker places a rootkit by:

- **Scanning** for vulnerable computers and servers on the web
- Wrapping **rootkit** in a special package like games
- Installing rootkit on the **public computers** or corporate computers through social engineering
- Launching zero day attack (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)
- Means of a link and a **bot** from IRC, ICQ, etc.

The primary purpose of a rootkit is to allow an attacker repeated **unregulated** and **undetected** access to a **compromised system**. Installing a backdoor process or replacing one or more of the files that run the normal connection processes can help meet this objective.

Attackers use rootkits to:

- Root the host system and gain remote backdoor access
- Mask attacker tracks and presence of **malicious applications** or processes
- Gather sensitive data, network traffic, etc. from the system to which attackers might be restricted or possess no access
- Store other malicious applications and act as a server resource for bot updates and so on



Types of Rootkits

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

Hypervisor-level Rootkit

Hypervisor-level rootkits are usually created by **exploiting hardware** features such as **Intel VT and AMD-V**. These rootkits host the operating system of the target machine as a virtual machine and intercept all hardware calls made by the **target operating system**. This kind of rootkit works by modifying the **system's boot sequence** and gets loaded instead of the original virtual machine monitor.

Kernel-level Rootkit

The kernel is the core of the operating system. These cover backdoors on the computer and are created by writing additional code or by substituting portions of **kernel code** with modified code via device drivers in Windows or **loadable kernel module** in Linux. If the kit's code contains mistakes or bugs, the stability of the system is greatly affected by the kernel-

level rootkits. These have the same privileges of the operating system, hence they are difficult to detect and intercept or subvert operations of operating systems.

Application-level Rootkit

Application-level **rootkit** operates inside the victim's computer by replacing the standard application files with rootkits or by **modifying** present applications with patches, injected code, etc.

Hardware/Firmware Rootkit

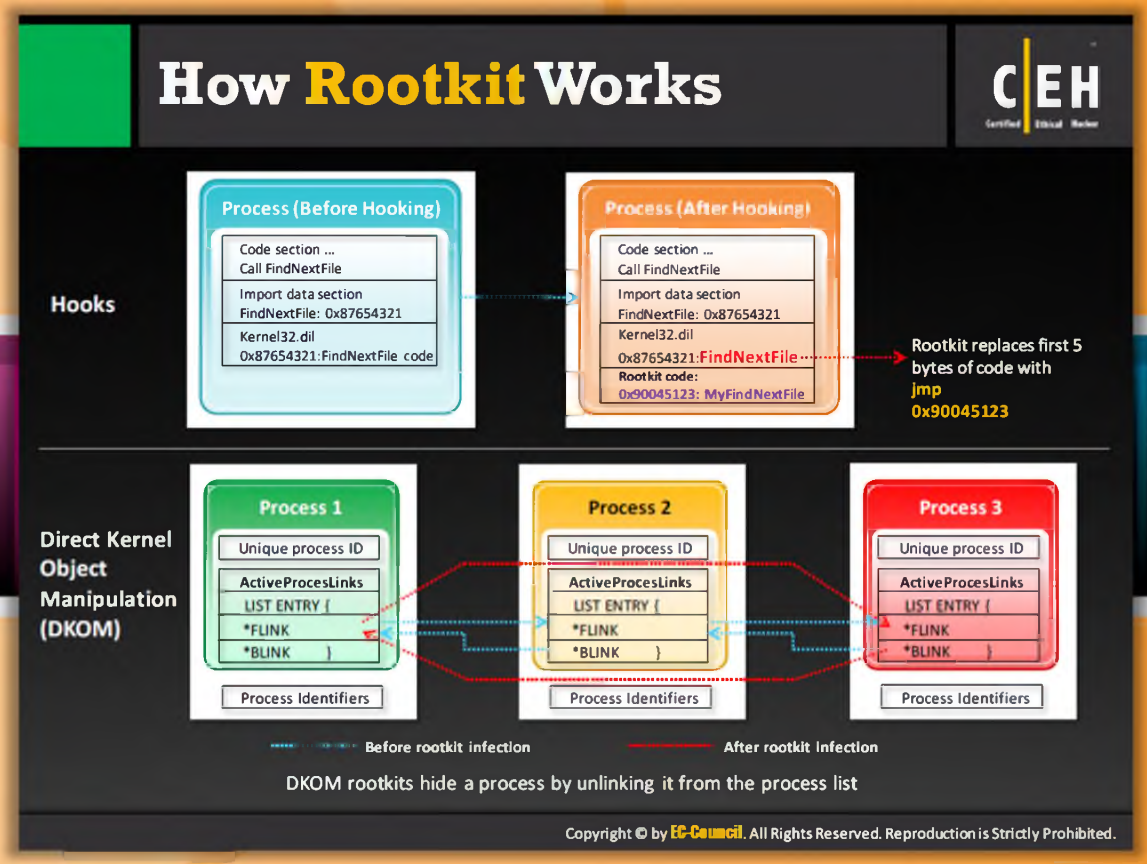
Hardware/firmware rootkits use devices or **platform firmware** to create a persistent malware image in hardware, such as a hard drive, system BIOS, or network card. The rootkit hides in firmware because firmware is not usually inspected for code integrity. A firmware rootkit implies the use of creating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

Boot-loader-level Rootkit (Bootkit)

Boot-loader-level (bootkit) rootkits function either by replacing or modifying the legitimate boot loader with another one. The boot-loader-level (bootkit) can be activated even before the operating system is started. So, boot-loader-level (bootkit) rootkits are serious threats to security because they can be used to **hack 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.



How Rootkits Work

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.

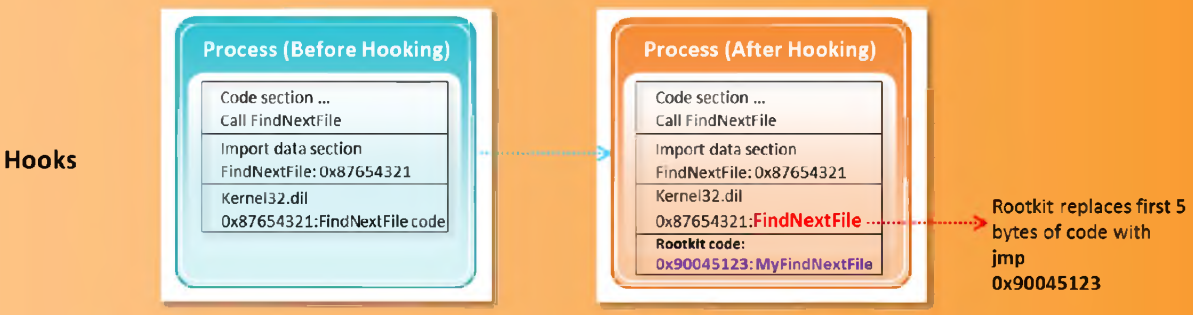


FIGURE 5.56: How Rootkits Work

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.

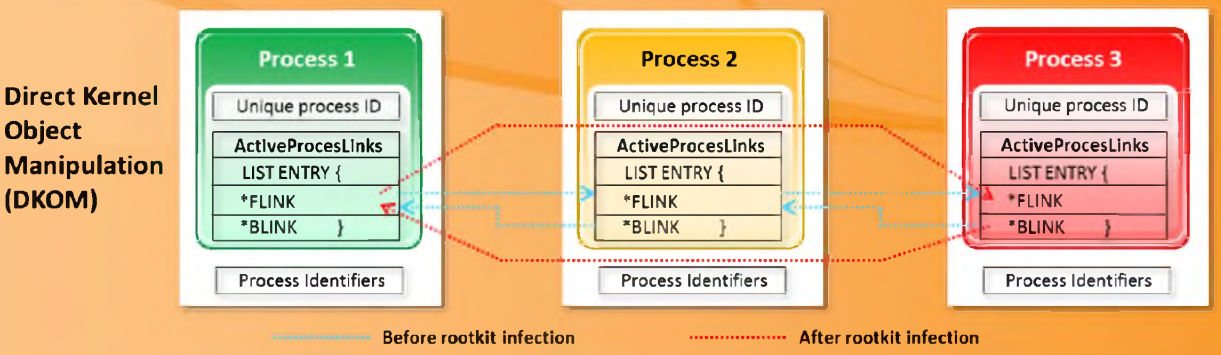
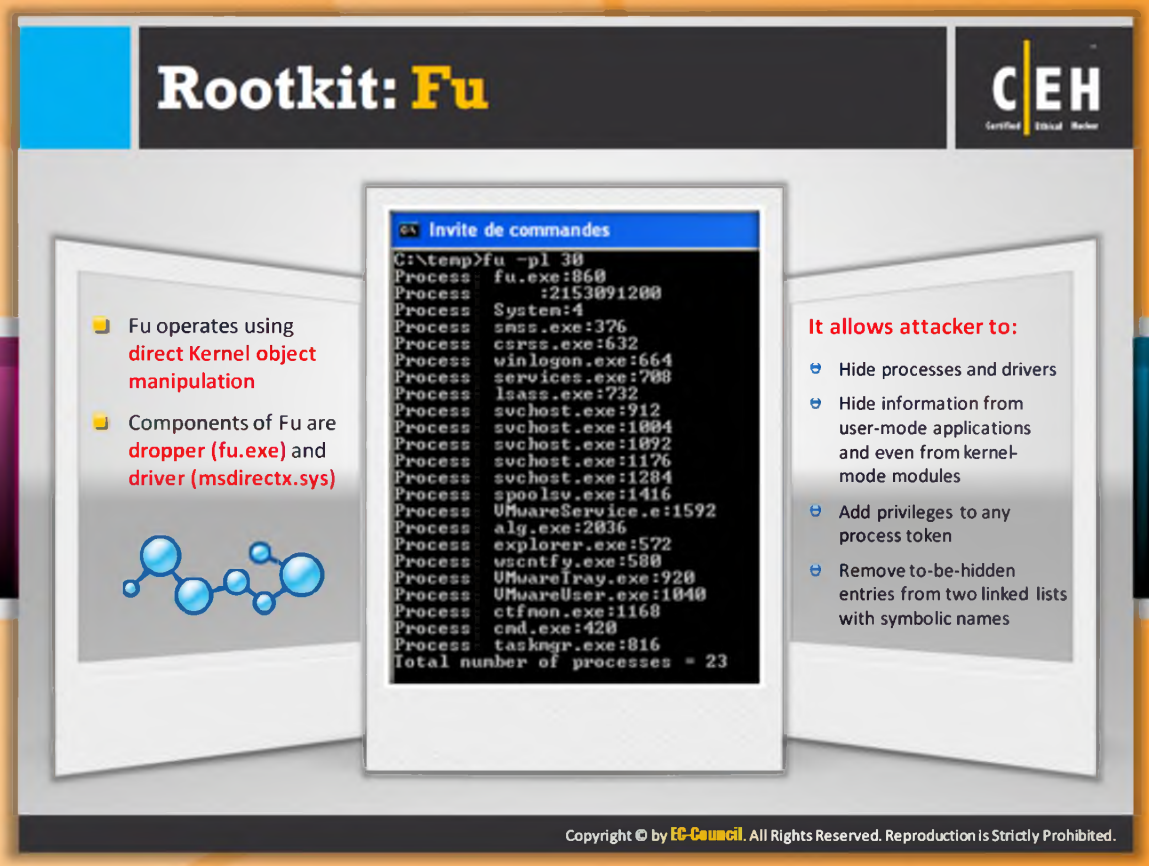


FIGURE 5.57: DKOM Rootkits Diagram



Rootkit: Fu

Fu is an infection database that operates using **Direct Kernel Object Manipulation** (DKOM) and comes with two components, the dropper (fu.exe) and the driver (msdirectx.sys). The Fu rootkit modifies the kernel object that represents the processes on the system. All the kernel process objects are linked. When a user process such as **TaskMgr.exe** requests the operating system for the list of processes through an API, Windows walks the linked list of process objects and returns the appropriate information. **Fu unlinks** the process object of the process it is hiding. Therefore, as far as many applications are concerned, the process does not exist.

The Fu rootkit can also allow you to hide and list processes and drivers by using different hooking techniques. It can add **privileges** to any process token. This can perform many actions in the **Windows event viewer** and appear as someone else's.

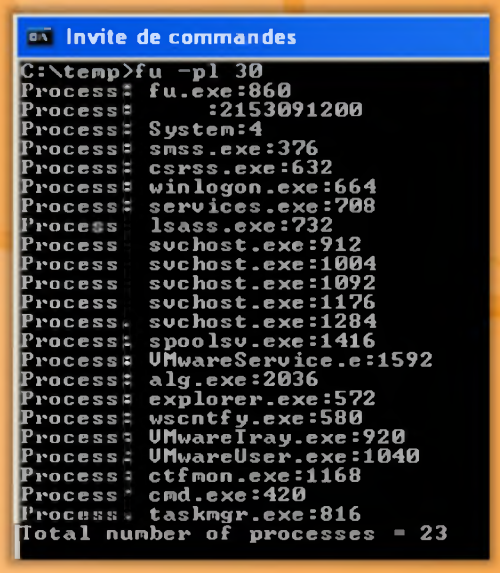
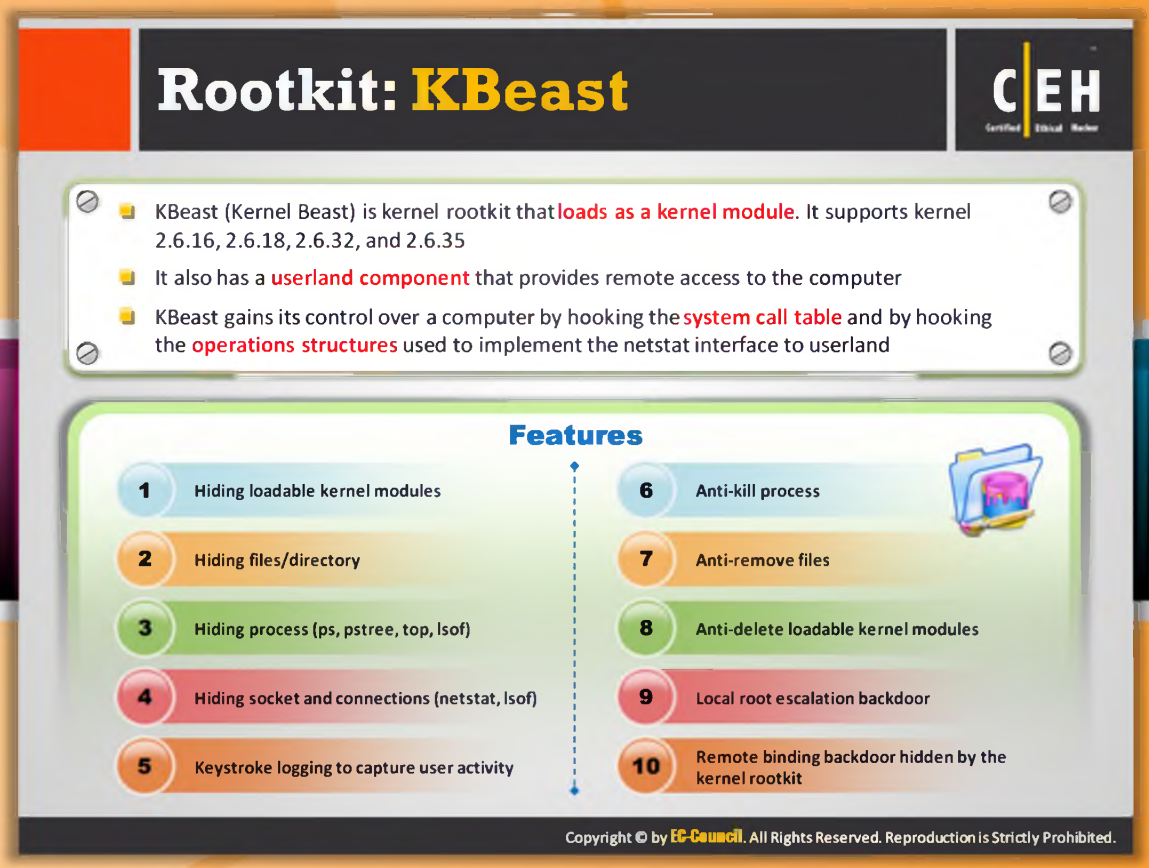


FIGURE 5.58: Fu in Command Promt



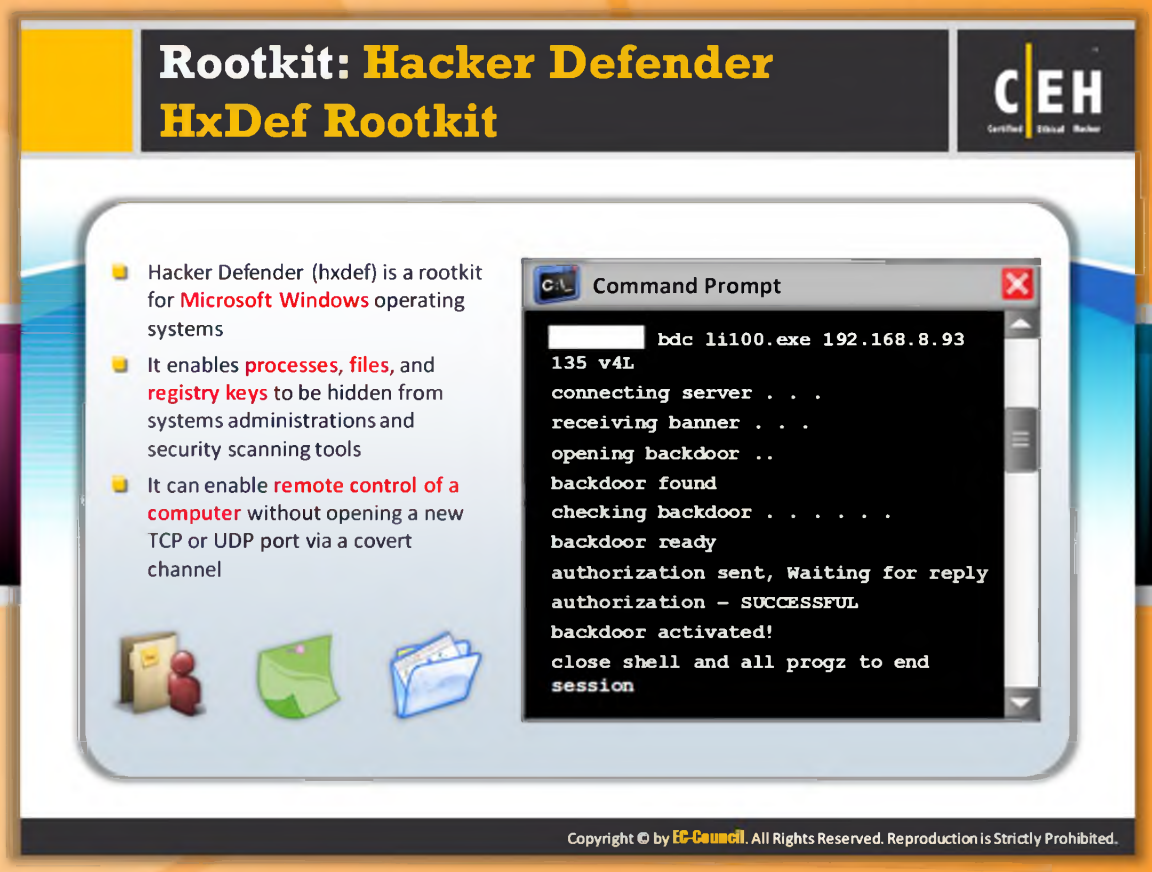
Rootkit: KBeast

KBeast (Kernel Beast) is kernel rootkit that loads as a kernel module. It supports kernel 2.6.16, 2.6.18, 2.6.32, and 2.6.35. It provides **remote access** to the systems by using its userland component. Using the kernel module, the userland backdoor component can be invisible from other userland applications. This can hide files, directories, and processes (ps, pstree, top, lsof) that start with a user-defined prefix. You can use keylogging abilities to capture the user activities. To implement the netstat interface to userland, KBeast obtains access over the system by **hooking** the system call table and operations structures.

The features of this rootkit include:

- Hiding this loadable kernel module
- Hiding files/directory
- Hiding process (ps, pstree, top, lsof)
- **Hiding** socket and connections (netstat, lsof)
- **Keystroke logging** to capture user activity
- Anti-kill process
- Anti-remove files

- Anti-delete this loadable kernel modules
- Local root **escalation backdoor**
- Remote binding backdoor **hidden** by the **kernel rootkit**



Rootkit: Hacker Defender HxDef Rootkit

Hacker Defender is a user-mode rootkit that modifies several Microsoft Windows operating systems and Native API functions. You can hide information like files, processes, and registry keys from **security scanning tools** and other applications. You can control a computer without opening a new TCP or UDP port via a covert channel from a remote area. It can also implement a backdoor and port redirector that can work through existing open **TCP ports**. Using its **stealth mode**, attackers can hide data from user-defined applications such as registry key values, allocated memory, system services, and drivers.

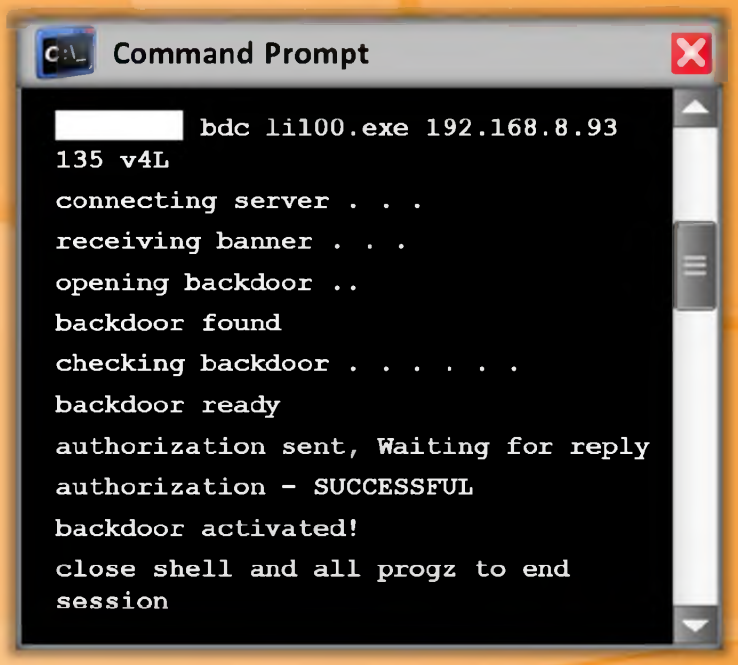
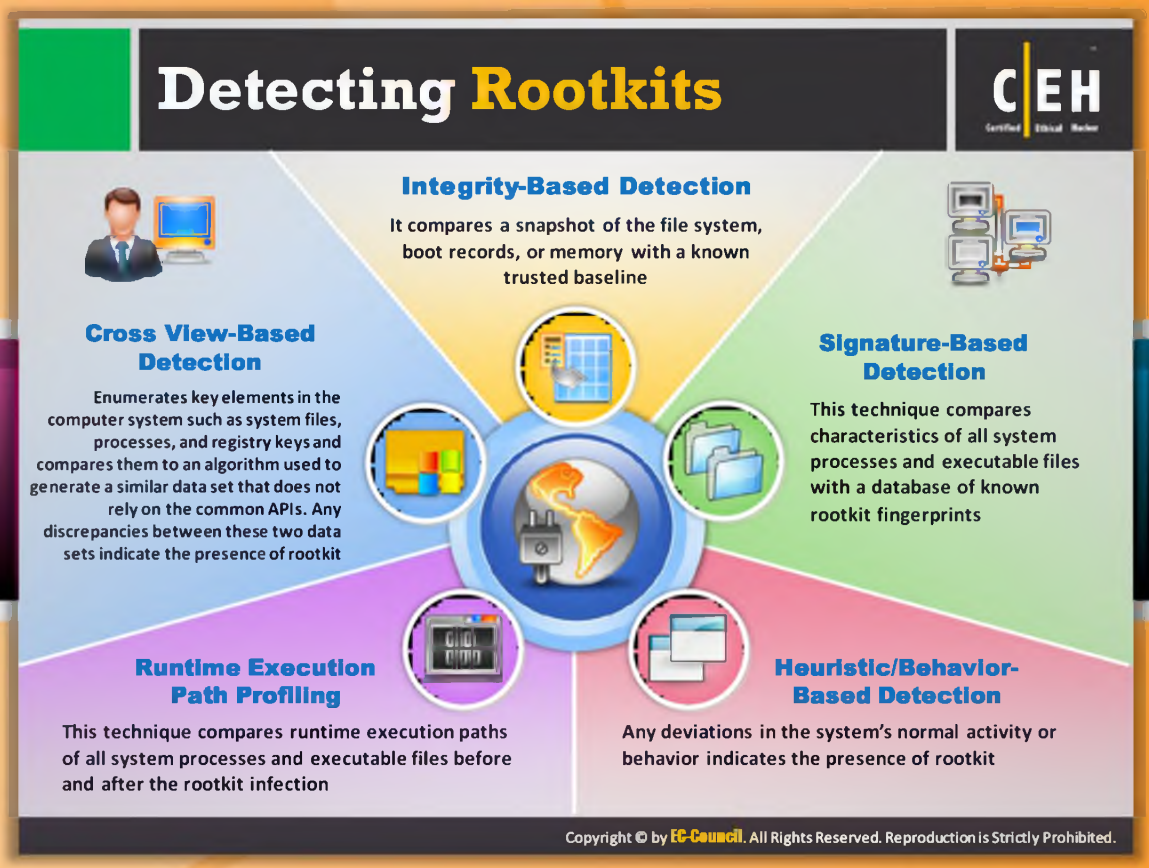


FIGURE 5.59: Hacker Defender HxDef Rootkit in Command Promt



Detecting Rootkits

The rootkit detection techniques are classified as signature, heuristic, integrity, cross-view-based, and **Runtime Execution Path Profiling**.

Signature-based Detection

Signature-based detection methods work as a **rootkit fingerprints**. You can compare the sequence of bytes from a file compared with another sequence of bytes that belong to a malicious program. This technique is mostly employed on system files. **Rootkits** that are invisible can be easily detected 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 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.

Integrity-based Detection

Integrity-based detection functions by comparing a current file system, boot records, or memory snapshot with a known, trusted baseline. The evidence or presence of malicious activity can be noticed by the dissimilarities between the current and baseline snapshots.

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 gathered information is then compared 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.

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, in order to destabilize it. The number of instructions executed before and after a certain routine is hooked and can be **significantly different.**

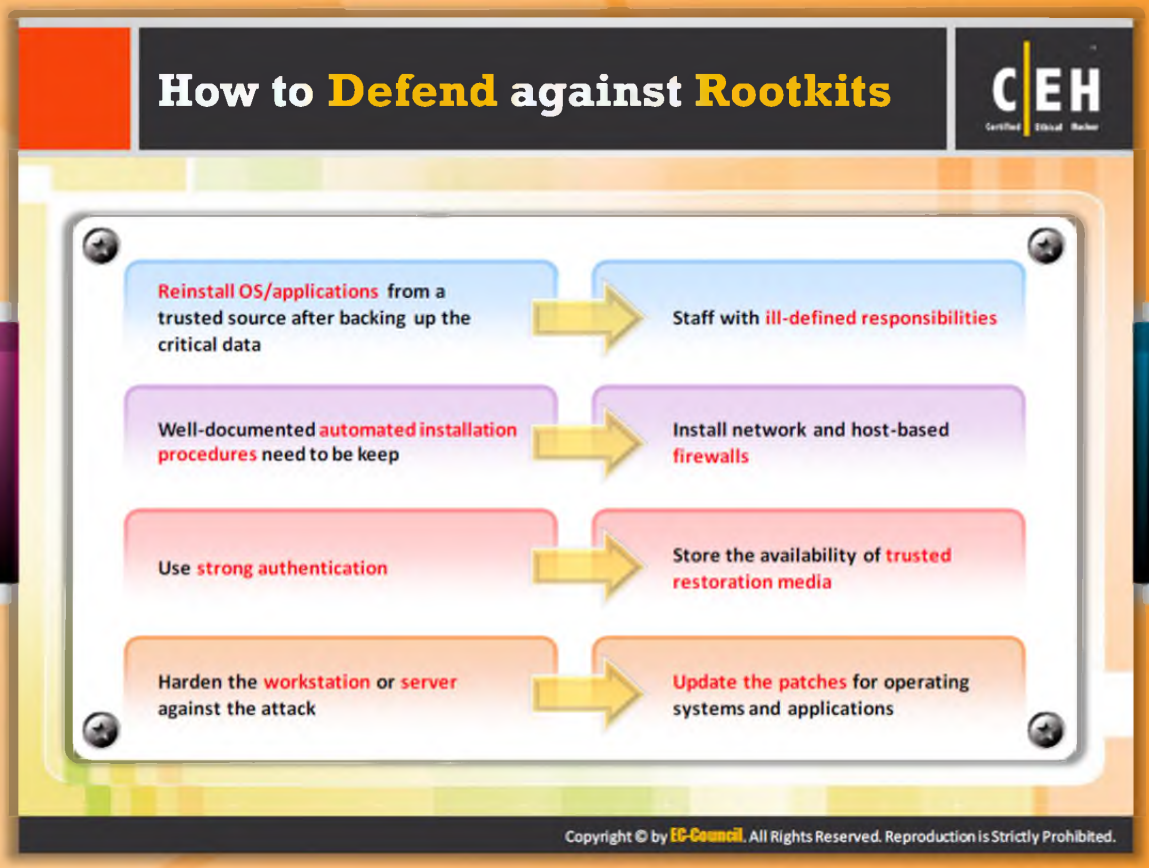
Steps for Detecting Rootkits

Source: http://research.microsoft.com

Follow these **steps to detect rootkits**:

1. Run "dir /s /b /ah" and "dir /s /b /a-h" inside the potentially infected OS and save the results.
2. Boot into a clean CD, run "dir /s /b /ah" and "dir /s /b /a-h" on the same drive, and save the results.
3. Run a clean version of WinDiff from the CD on the two sets of results to detect file-hiding ghostware (e.g., 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, etc.



How to Defend against Rootkits

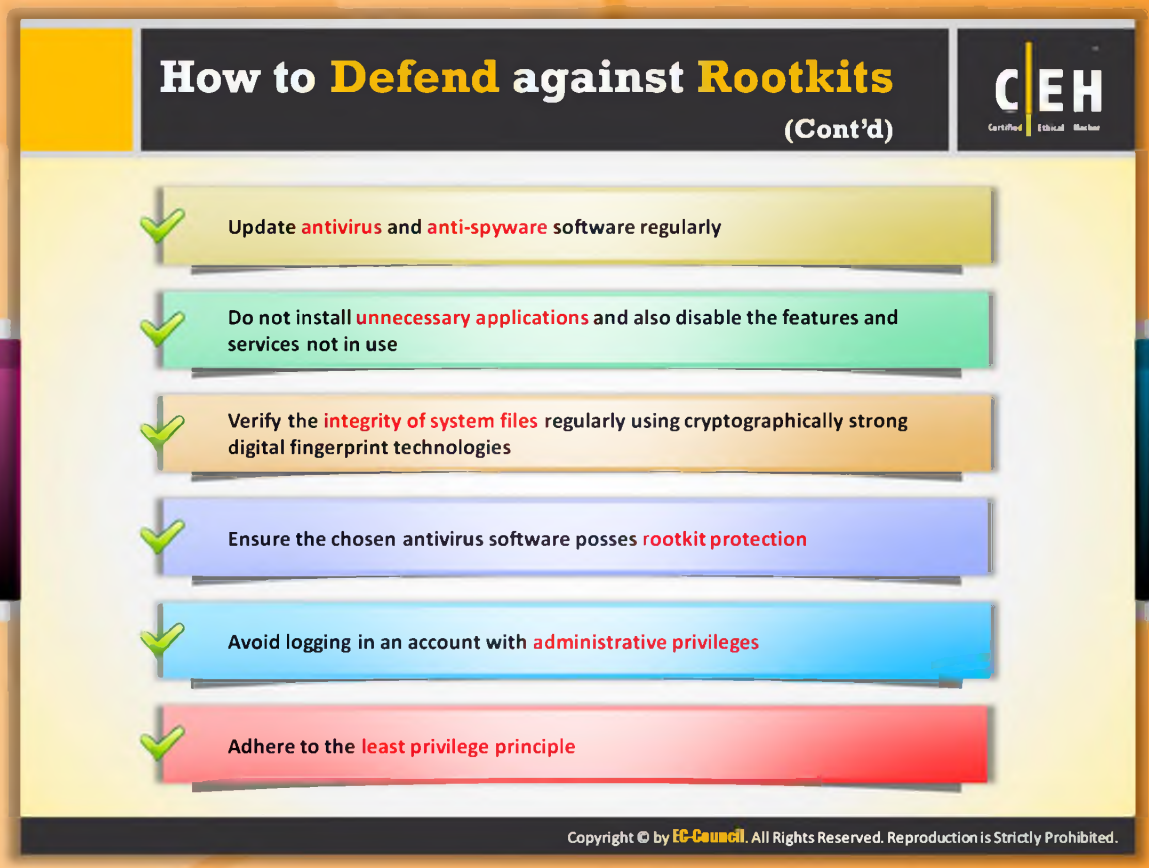
A common feature of these rootkits is that the attacker requires administrator access to the target system. The **initial attack** that leads to this access is often noisy. Excess network traffic that arises in the face of a new exploit should be monitored. It goes without saying that log analysis is 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**, integrity checking programs for critical system files can be used. Numerous tools, programs, software, and techniques are available to check for **rootkits**.

A few techniques that are adopted to defend against rootkits are listed as follows:

- Reinstall OS/applications from a trusted source after backing up the critical data
- Staff with ill-defined responsibilities
- Well-documented **automated installation** procedures need to be keep

- Install network and host-based firewalls
- Use **strong authentication**
- Store the availability of trusted restoration media
- Harden the workstation or server against the attack
- Update the **patches** for operating systems and applications

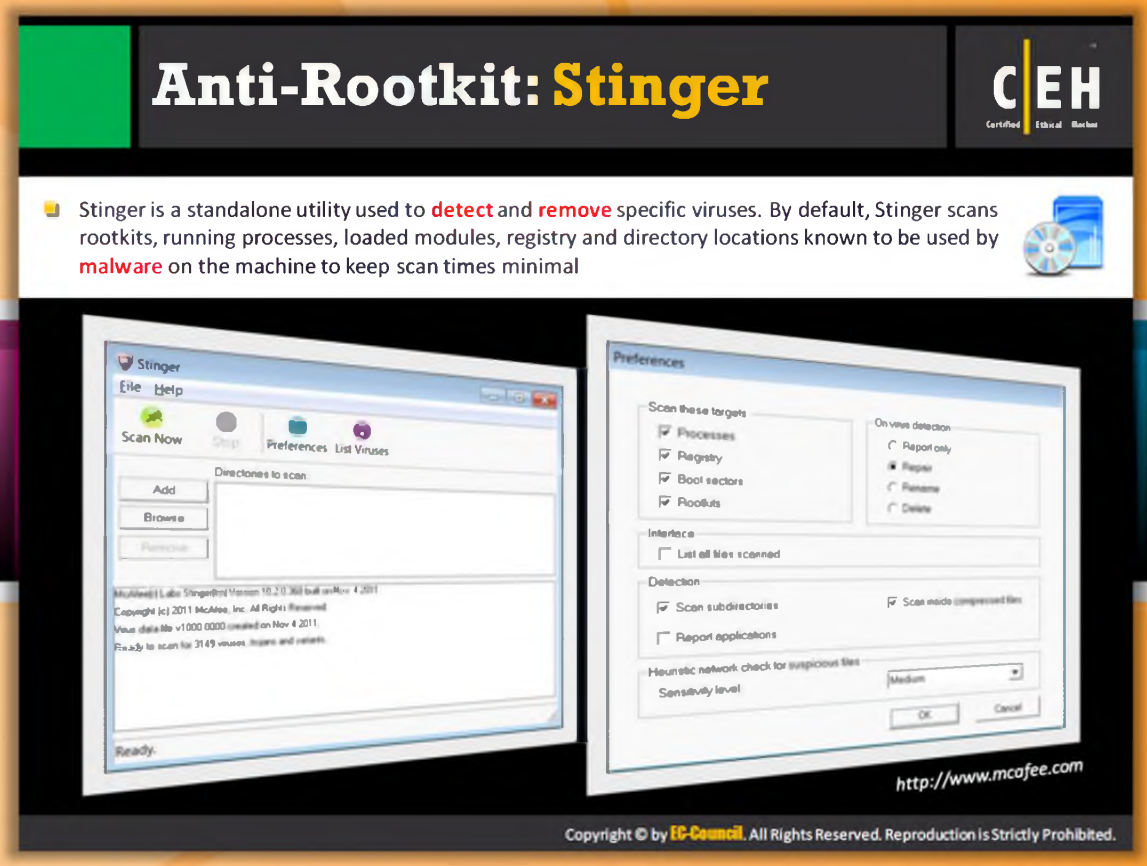


How to Defend against Rootkits (Cont'd)

Now you have seen **basic countermeasures** for defending against rootkits there are some more countermeasures that will assist you in defending against rootkits.

Let's take look at what more you can do to defend against rootkit.

- You should update you antivirus and antispyware software regularly
- You should not install unnecessary applications on your system and also disable the features and services not in use
- You should verify the **integrity** of system files regularly using **cryptographically** strong digital fingerprint technologies
- Ensure that the chosen antivirus software possesses rootkit protection before it is installed
- You should avoid logging in an account with administrative privileges
- You should adhere to the **least privilege** principle



Anti-Rootkit: Stinger

Source: http://www.mcafee.com

McAfee Stinger helps you to detect and remove **prevalent Fake Alert malware**, viruses, and threats identified in your system. Stinger scans rootkits, **running** processes, loaded modules, the registry, and directory locations known to be used by malware on the machine to keep scan times minimal. It can also repair the **infected files** found in your system. It detects and deactivates all the viruses from your system.

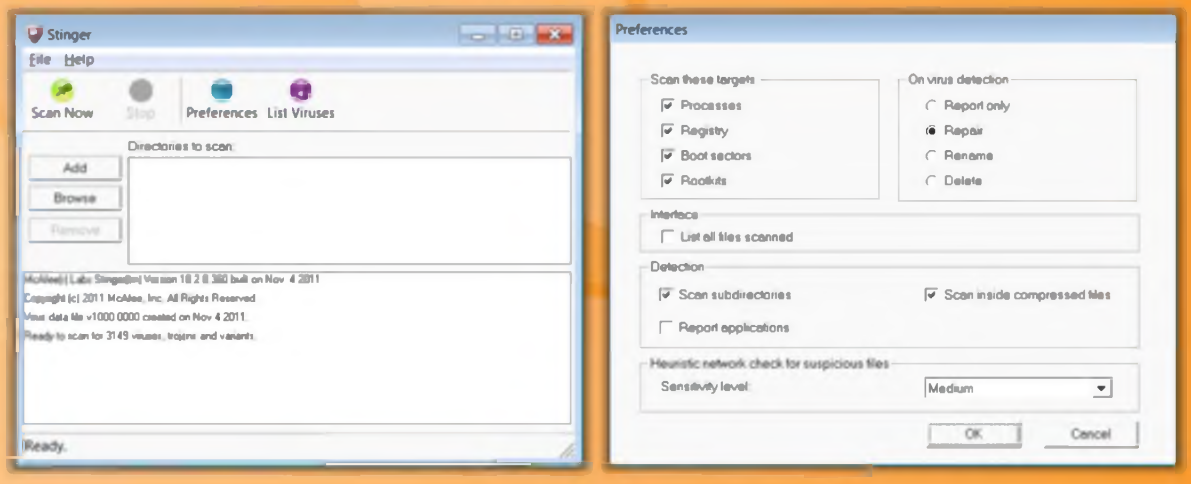
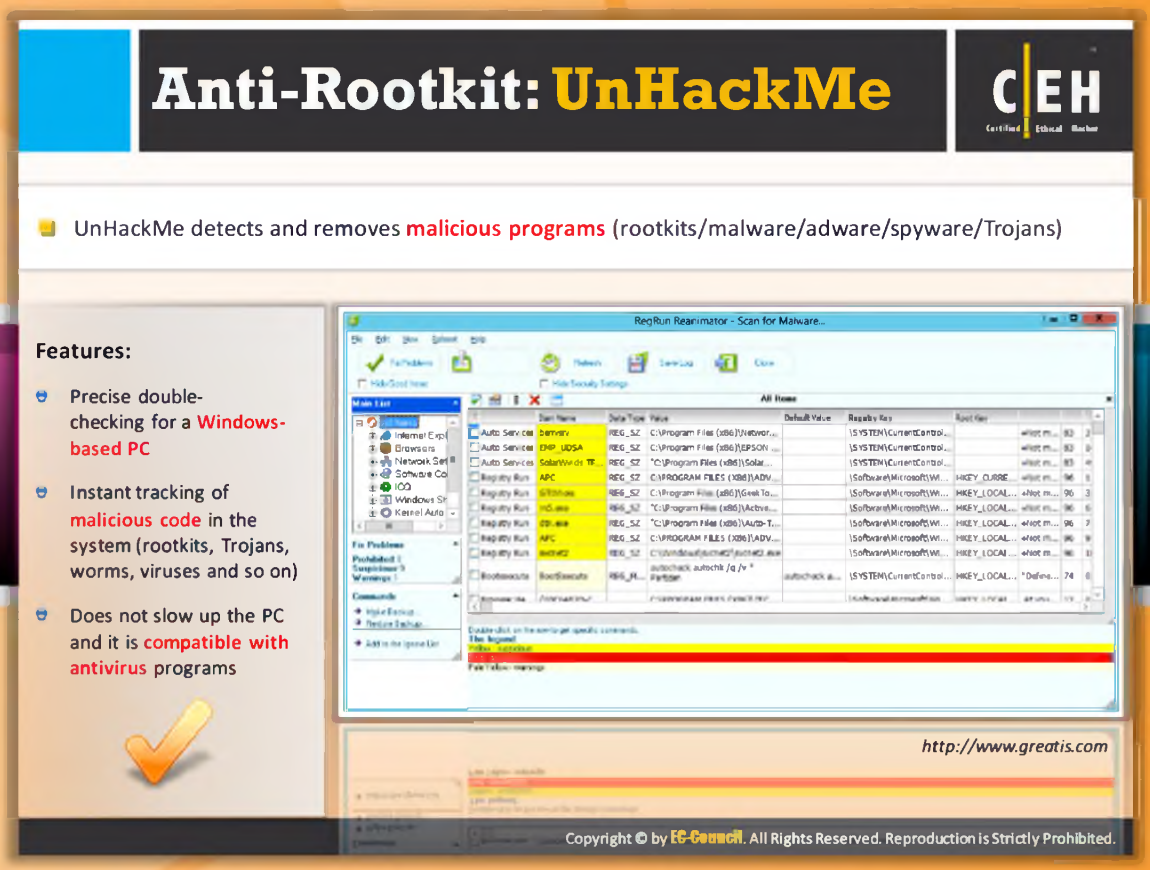


FIGURE 5.60: Stinger Screenshot



Anti-Rootkit: 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.

Features:

- Precise double-checking for a Windows-based PC
- Instant tracking of **malicious code** in the system (rootkits, Trojans, worms, viruses and so on)
- Does not slow up the PC and it is compatible with **antivirus programs**

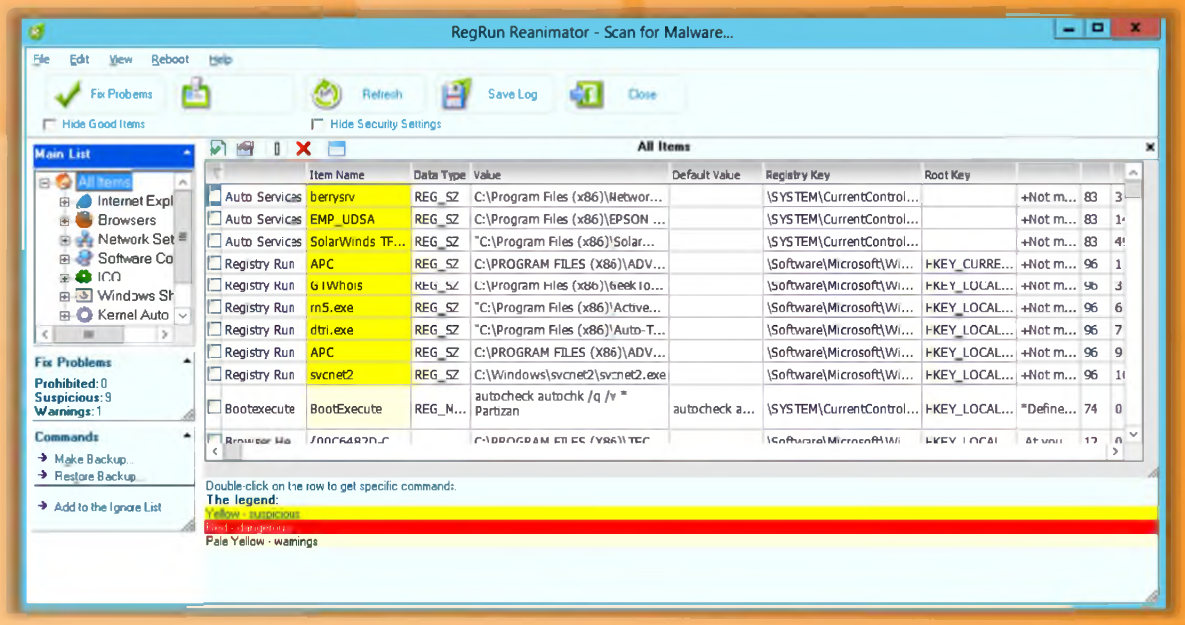
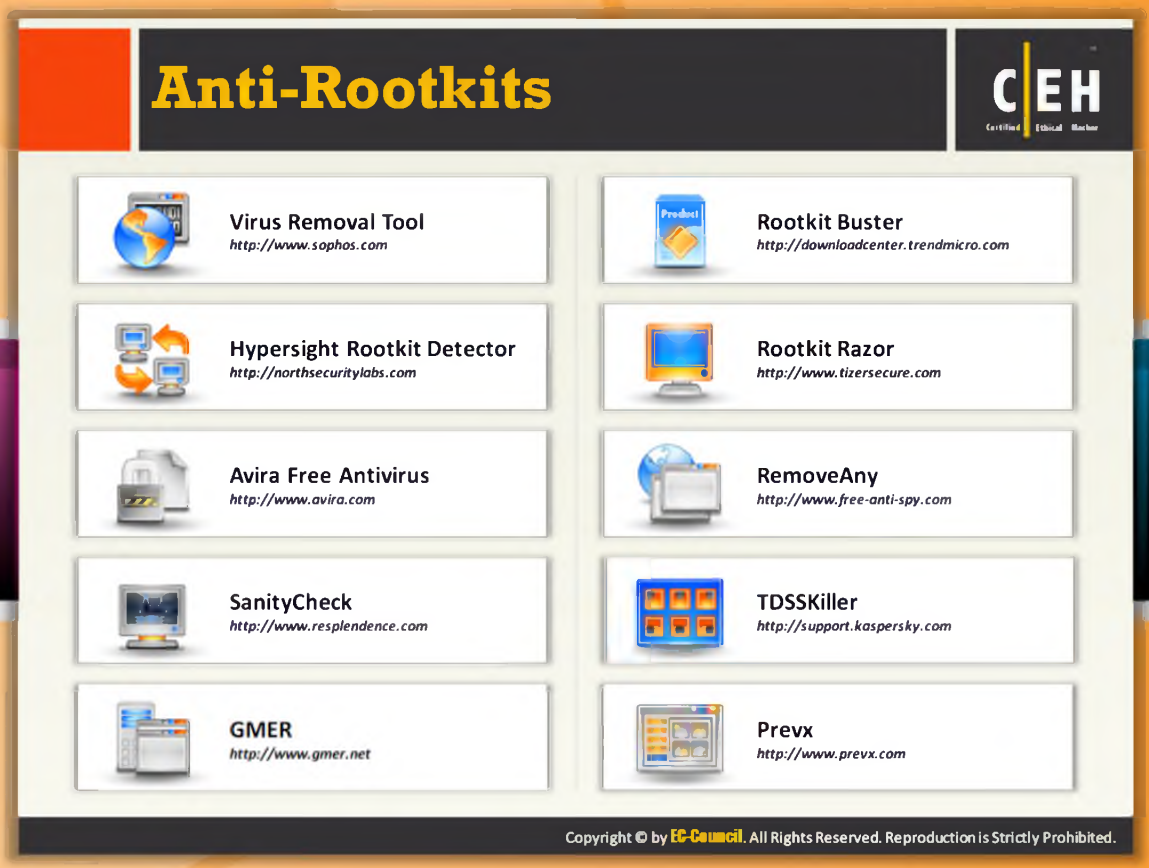


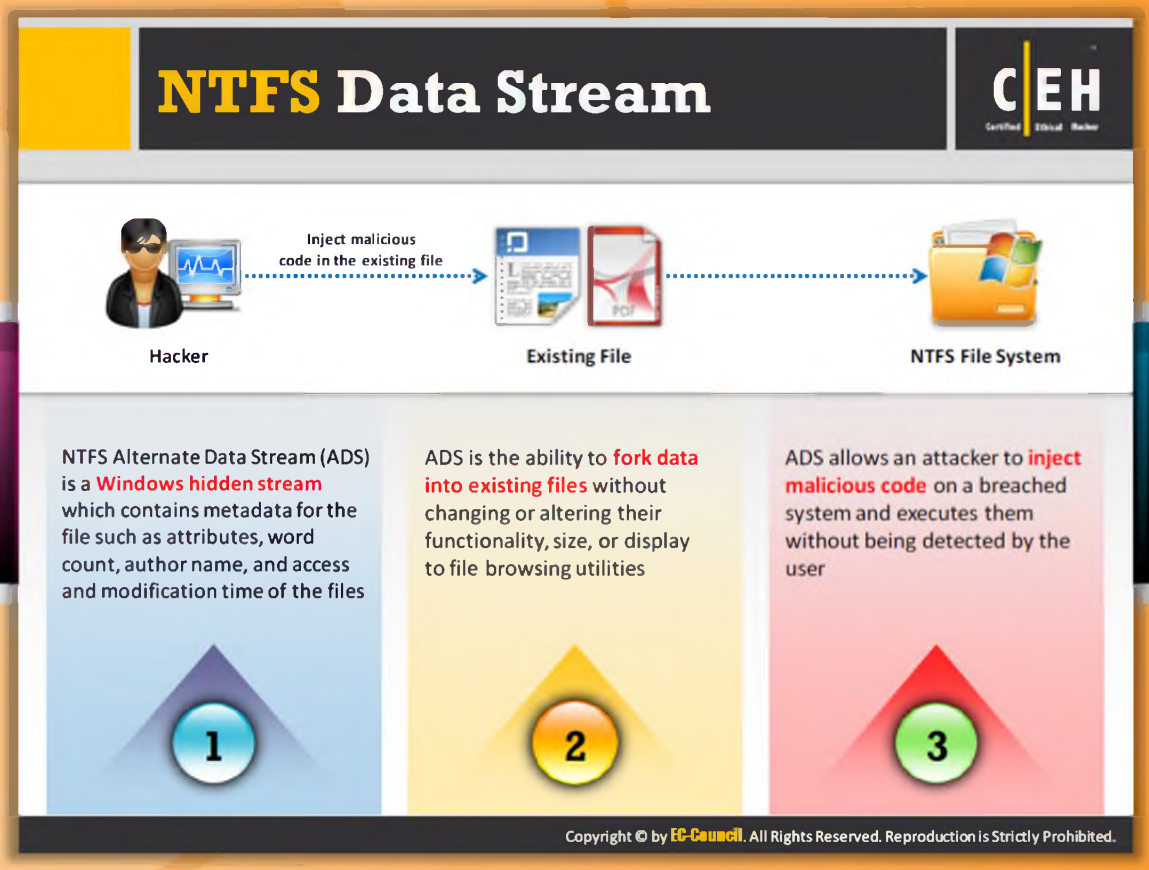
FIGURE 5.61: UnHackMe Screentshot



Anti-Rootkits

The following anti-rootkits 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 home sites and install it on your PC to be **protected** from rootkits. A few **anti-rootkits** are listed as follows:

- Virus Removal Tool available at http://www.sophos.com
- Hypersight Rootkit Detector available at http://northsecuritylabs.com
- Avira Free Antivirus Tool available at http://www.avira.com
- SanityCheck available at http://www.resplendence.com
- GMER available at http://www.gmer.net
- Rootkit Buster available at http://downloadcenter.trendmicro.com
- Rootkit Razor available at http://www.tizersecure.com
- RemoveAny available at http://www.free-anti-spy.com
- TDSSKiller available at http://support.kaspersky.com
- Prevx available at http://www.prevx.com



NTFS Data Stream

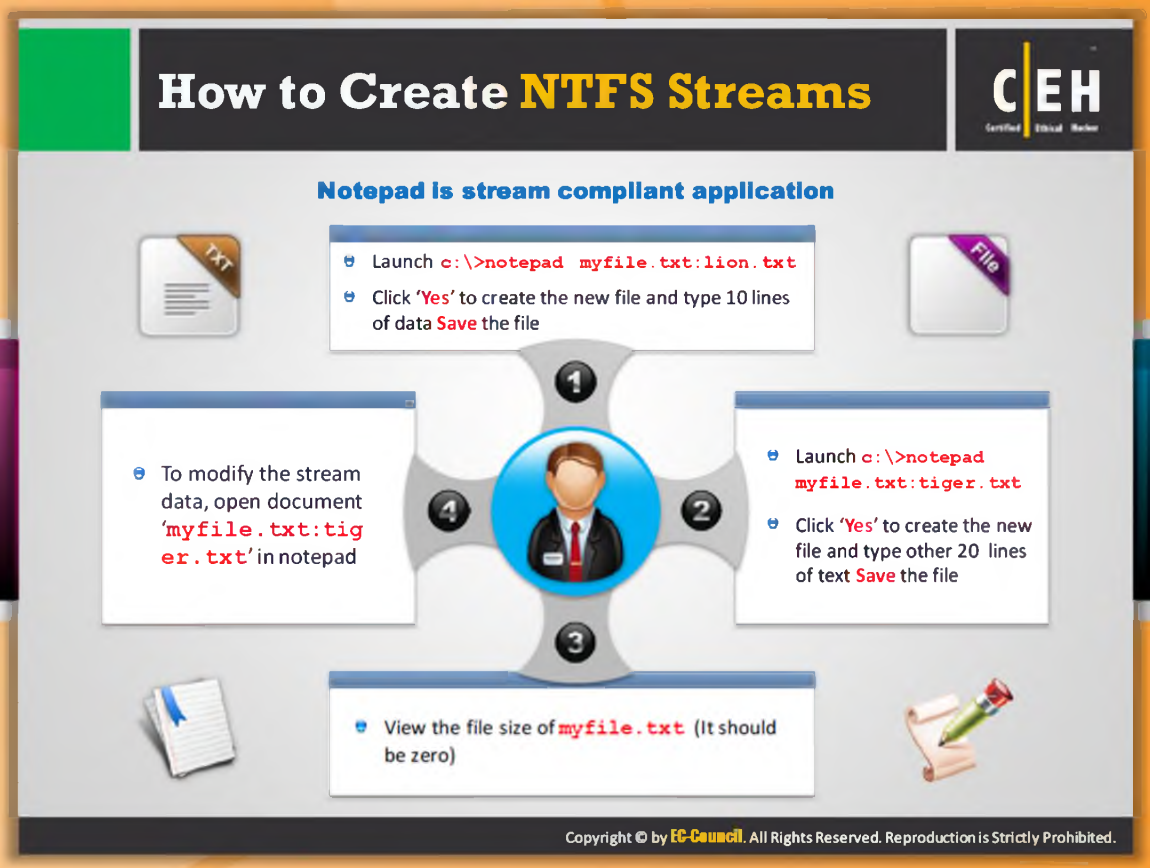
In addition to the file attributes, each file stored on an NTFS volume typically contains two data streams. The first data stream stores the security descriptor, and the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

Alternate Data Stream (ADS) is any kind of data that can be 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 them to be executed without being detected by the system's administrator. Files with ADS are impossible to detect using native file browsing techniques like the command line or **Windows Wxplorer**. 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 anyfile.exe. The only indication that the file was changed is the **modification** time stamp, which can be relatively innocuous.

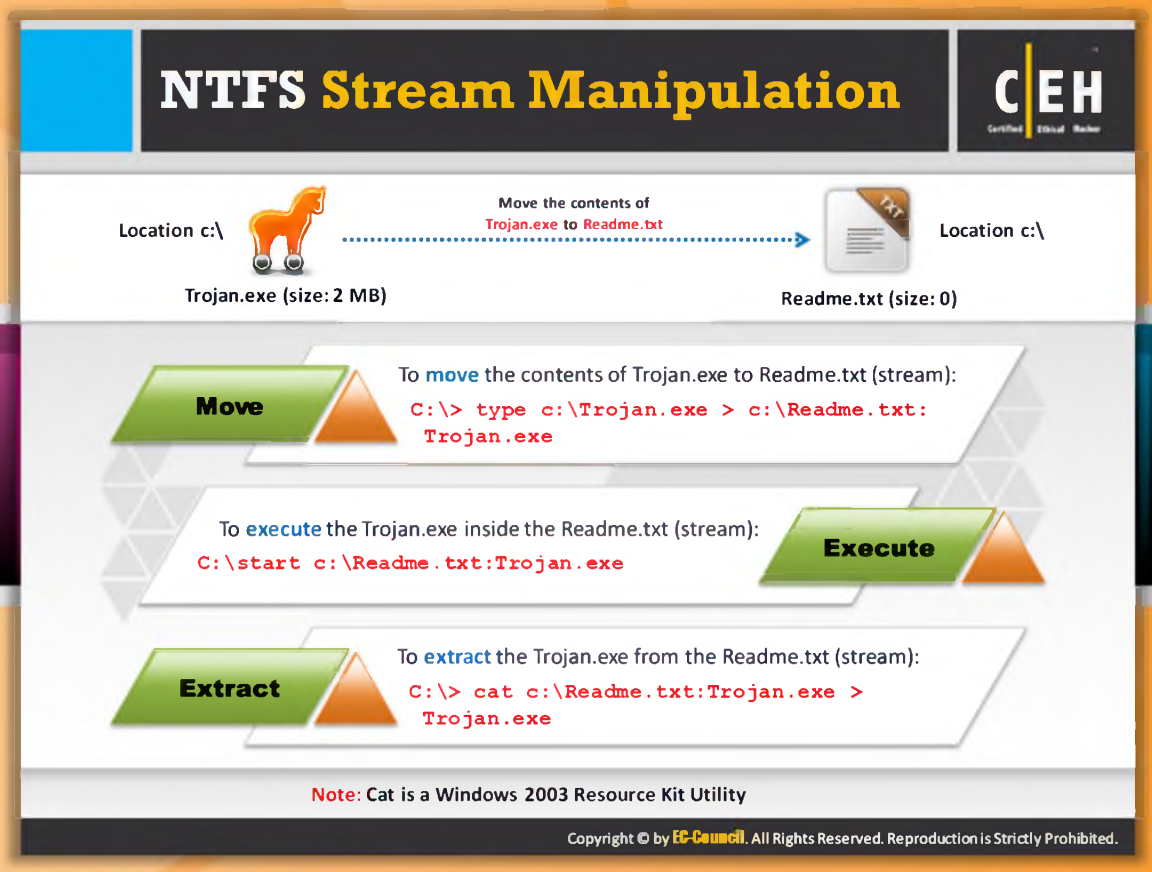
FIGURE 5.62: Working of NTFS Data Stream



How to Create NTFS Streams

You can create NTFS Streams by following these steps:

- Launch `c:\>notepad myfile.txt:lion.txt`
- Click **Yes** to create the new file and type 10 lines of data.
- Save the file.
- Launch `c:\>notepad myfile.txt:tiger.txt`
- Click **Yes** to create the new file and type other 20 lines of text
- Save the file.
- View the file size of `myfile.txt` (it should be zero).
- To modify the stream data, open the document '`myfile.txt:tiger.txt`' in Notepad.



NTFS Stream Manipulation

You can manipulate the NTFS streams by executing the following steps:

- To move the contents of Trojan.exe to Readme.txt (stream):

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

- To execute the Trojan.exe inside the Readme.txt (stream):

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

- To extract the Trojan.exe from the Readme.txt (stream):

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

Note: Cat is a Windows 2003 Resource Kit Utility.

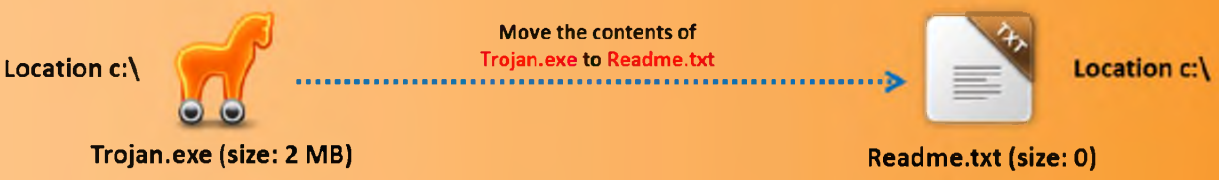
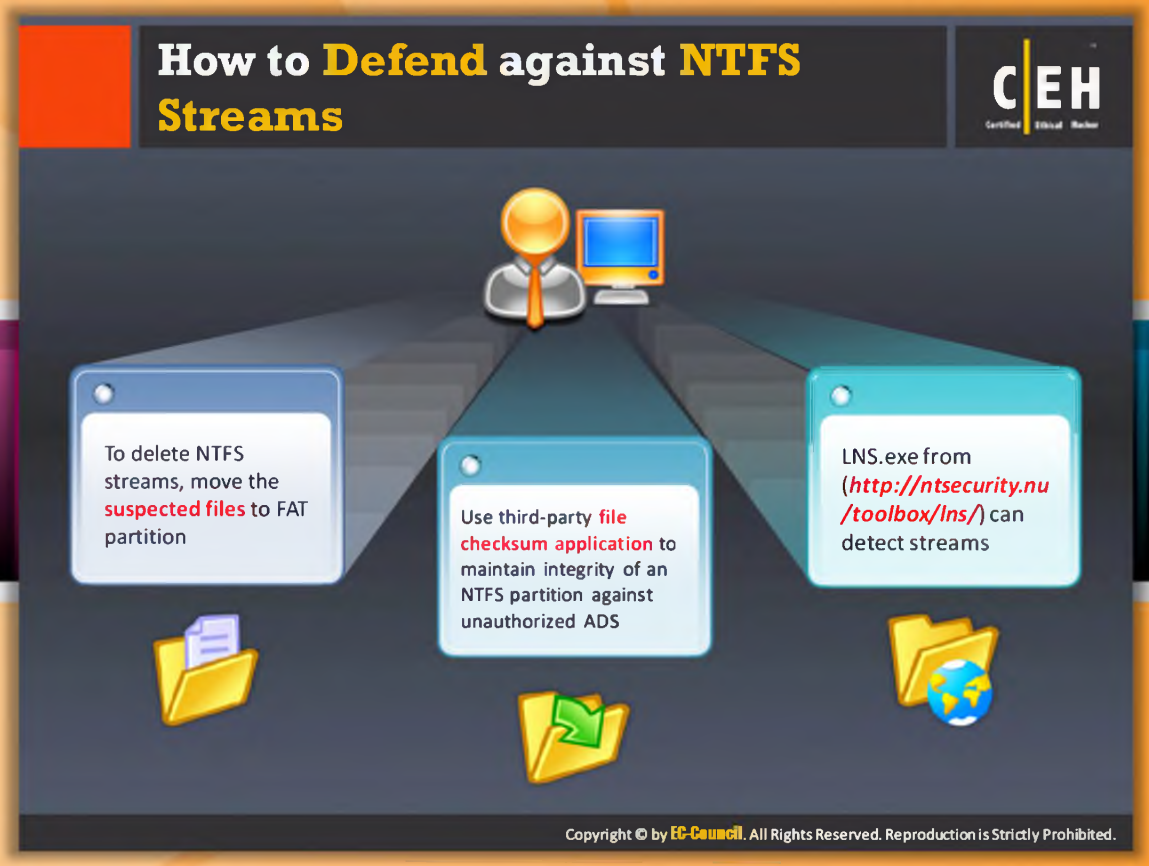


FIGURE 5.63: Working of NTFS Stream Manipulation



How to Defend against NTFS Streams

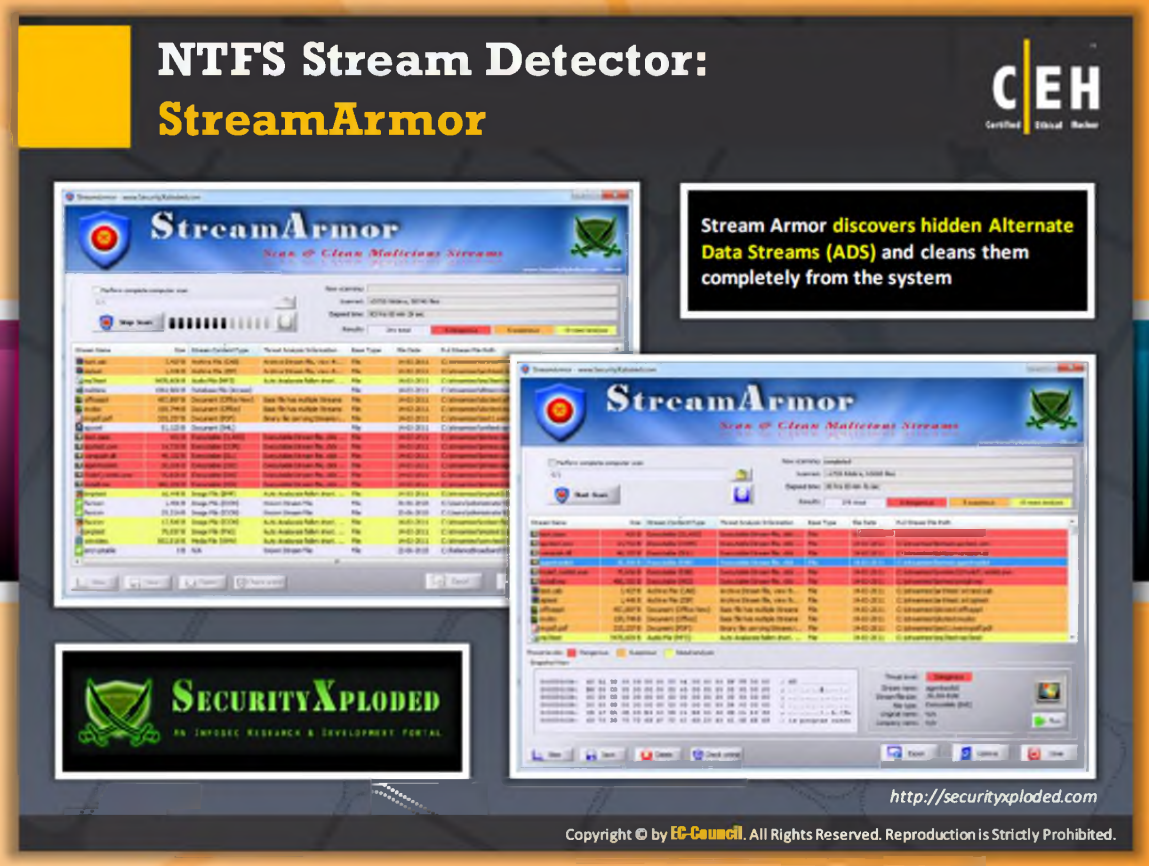
You should use **Lads.exe software** as a countermeasure for NTFS. The latest version of lads.exe gives you a report for the availability status of ADSs. Lad.exe is useful to administrators who deal with graphics since this tool provides the findings on the screen. This **tool searches** for either single or **multiple streams**. It provides a report of the ADSs' presence as well as gives the full path and length of each ADS that is found.

Other means include copying the cover file to a FAT partition and then moving it back to NTFS. This corrupts and loses the streams.

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

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

- Use **up-to-date** antivirus software on your system
- Enable real-time scanning of antivirus as it will protect from execution of malicious streams inside your system
- Use file monitoring software such **LAD**, as it helps you to detect creation of additional or new data streams

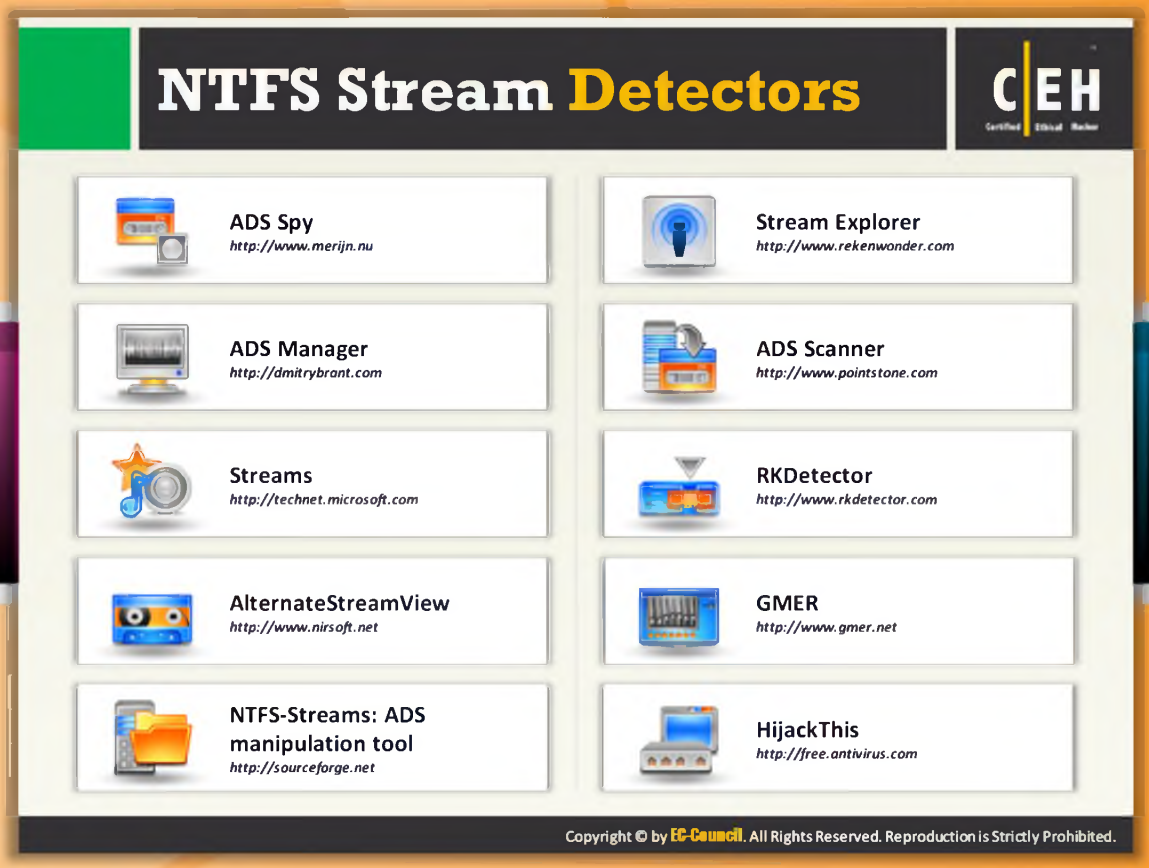


NTFS Stream Detector: StreamArmor

Source: http://securityxploded.com

This tool helps you to detect the hidden **Alternate Data Stream** (ADS) and remove it from your system completely. Its **multithreaded ADS scanner** helps you to scan recursively over the entire system and uncovers all the hidden streams from your system. You can easily detect the suspicious data stream from a normal data stream as it displays the discovered **specific stream** with a specific color pattern. It is also able to detect file the type of stream by using the **Advance File type detection mechanism**.

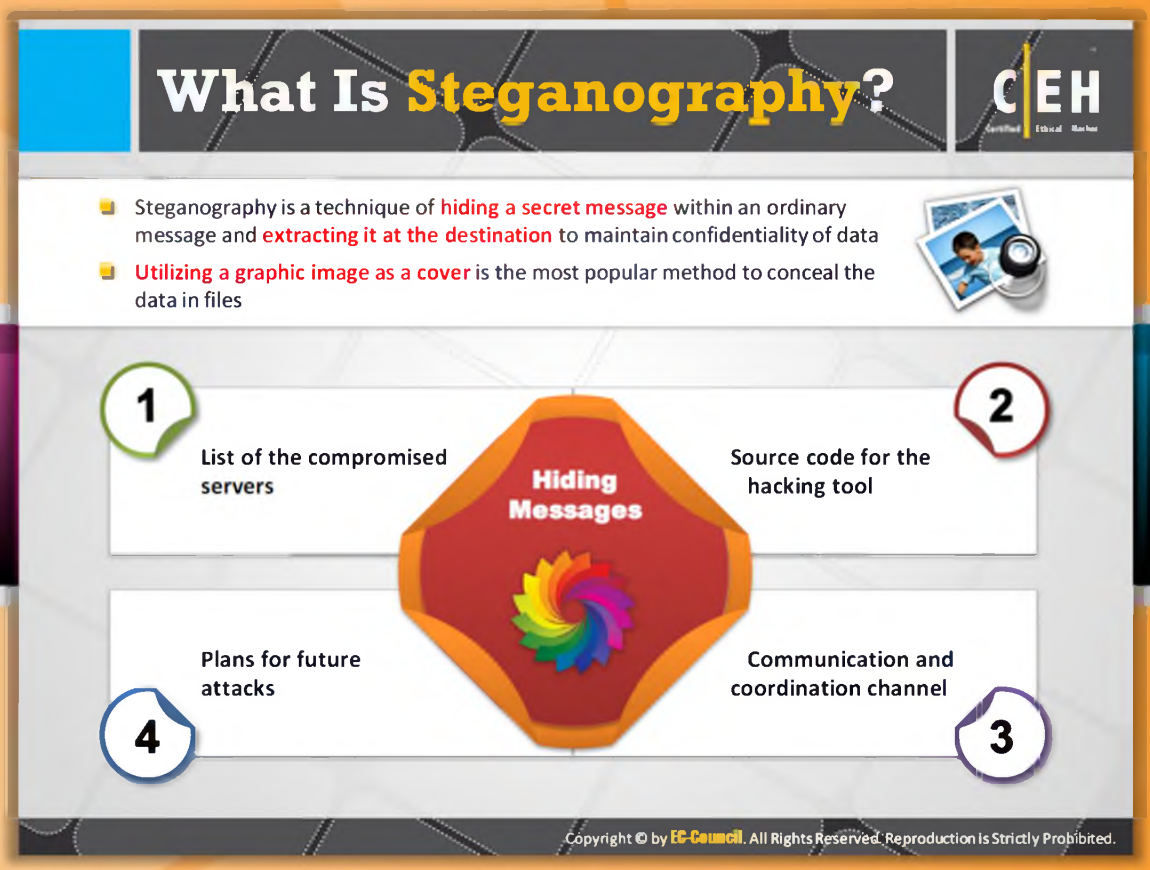
FIGURE 5.64: StreamArmor Screenshot



NTFS Stream Detectors

There are various NTFS Stream Detectors available in 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 available at http://www.merijn.nu
- ADS Manager available at http://dmitrybrant.com
- Streams available at http://technet.microsoft.com
- AlternateStreamView available at http://www.nirsoft.net
- NTFS-Streams: ADS manipulation tool available at http://sourceforge.net
- Stream Explorer available at http://www.rekenwonder.com
- ADS Scanner avaialble at http://www.pointstone.com
- RKDetector available at http://www.rkdetector.com
- GMER available at http://www.gmer.net
- HijackThis avaialble at http://free.antivirus.com



What is Steganography?

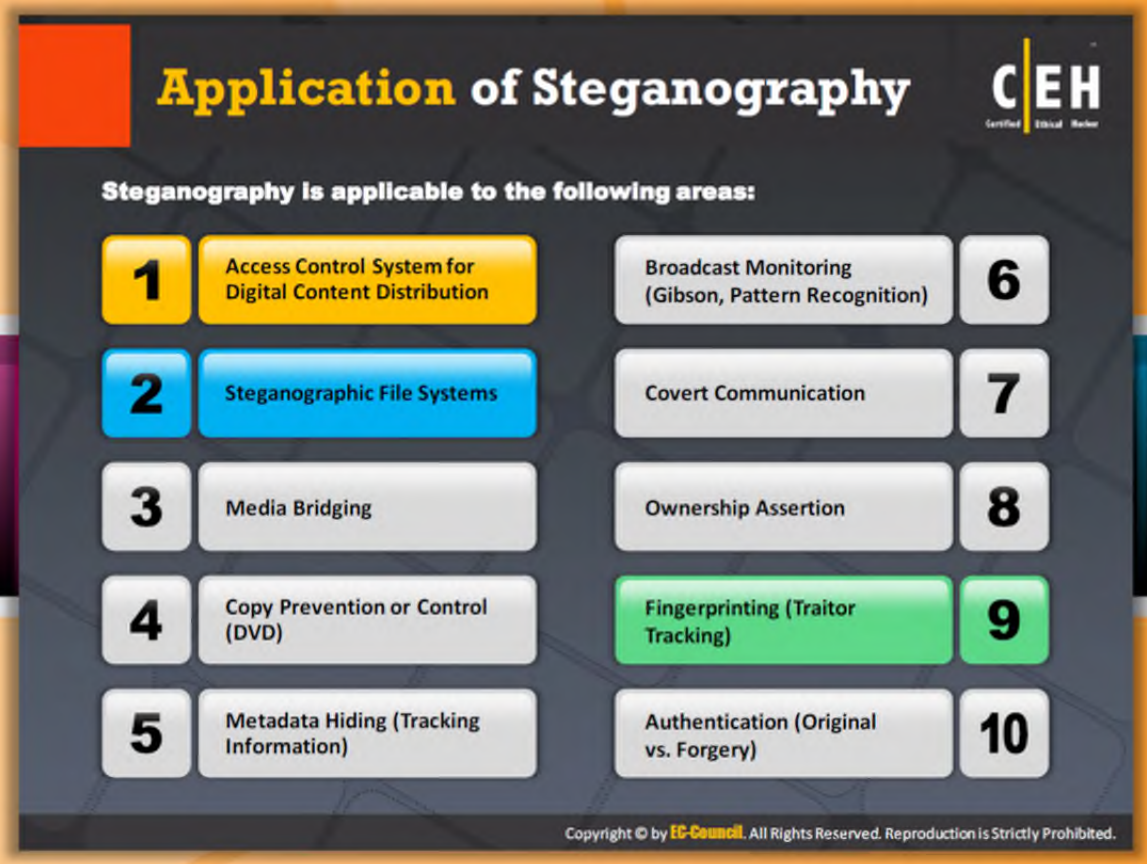
It has been argued that one of the **shortcomings** of various detection programs is their primary focus on streaming text data. What if an attacker bypasses normal surveillance techniques and still steals or **transmits** sensitive data? A typical situation would be where an attacker manages to get inside a firm as a temporary or contract employee and **surreptitiously** seeks out sensitive information. While the organization may have a policy of not allowing **electronic equipment** to be removed from a facility, a determined attacker can still find a way with techniques such as steganography.

Steganography is defined as the art of hiding data behind some other data without the knowledge of the enemy. It replaces bits of unused data into the usual files—**graphic, sound, text, audio, video**—with some other bits that have been obtained **surreptitiously**. The hidden data can be plaintext or ciphertext, or it can be an image.

The lure of the steganography technique is that, unlike encryption, steganography cannot be detected. When transmitting an encrypted message, it is evident that communication has occurred, even if the message cannot be read. Steganography is used to hide the existence of the message. An attacker can use it to hide information even when encryption is not a feasible option. From a security point of view, steganography is used to hide the file in an encrypted

format. This is done so that even if the file that is encrypted is decrypted, the message will still 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



Application of Steganography

The application of steganography differs in many areas and the area depends on what feature of steganography is utilized. Steganography is applicable to:

- **Access Control System for Digital Content Distribution**

  In the Access Control System for **Digital Content Distribution** system, the embedded data is "hidden," but is "explained" to publicize the content. In this system, a prototype of an Access Control System for digital content is developed to send data through the Internet. Using folder access keys, the content owner embeds the content in a folder and uploads on the web page. Here the content owner explains the content and publishes the contact details on the **World Wide Web** to get **an access-request from users** and they can contact him or her to get the access key. The valuable data can be protected using special access keys.

- **Steganography File Systems**

  A Steganography File System has a level of security using which hiding data is done by a series of fixed size files originally consisting of random bits on top of which vectors could be superimposed in such a way as to allow levels of security to decrypt all lower levels. Even the existence of any higher levels, or an entire partition, is filled with random bits and files hidden in it.

- **Media Bridging**

  Using digital **steganography**, electronic communications can by encrypted in the transport layer, such as a document file, image file, program, or protocol.

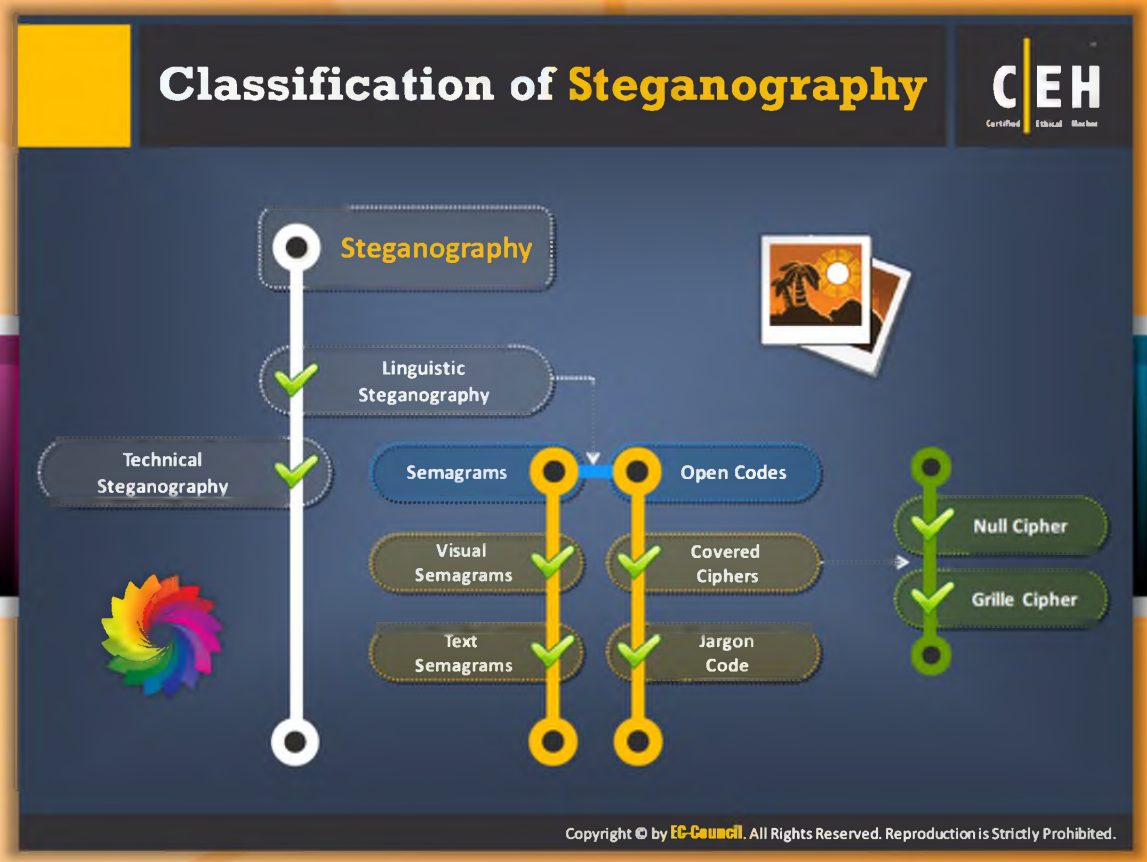
- **Copy Prevention or Control (DVD)**

  In the entertainment industry steganography can be used to protect copyrights for DVDs and CDs. The DVD **copy-protection** program is designed to support a copy generation management system.

- **Metadata Hiding (Tracking Information)**

  Metadata can be used to track geo location and to prevent or control copying digital material, i.e., **preventing unauthorized duplication** of digital data.

- **Broadcast Monitoring (Gibson, Pattern Recognition)**
- **Covert Communication**
- **Ownership Assertion**
- **Fingerprinting (Traitor Tracking)**
- **Authentication (Original vs. Forgery)**



Classification of Steganography

Steganography is classified into **two areas based on techniques**. They are technical steganography and linguistic steganography. Technical steganography hides a message using scientific methods, whereas the **linguistic steganography** hides the message in the carrier, a medium used to communicate or transfer messages or files. The steganography medium is usually defined as the combination of the hidden message, the carrier, and the steganography key. The following **diagram depicts** the classification of steganography.

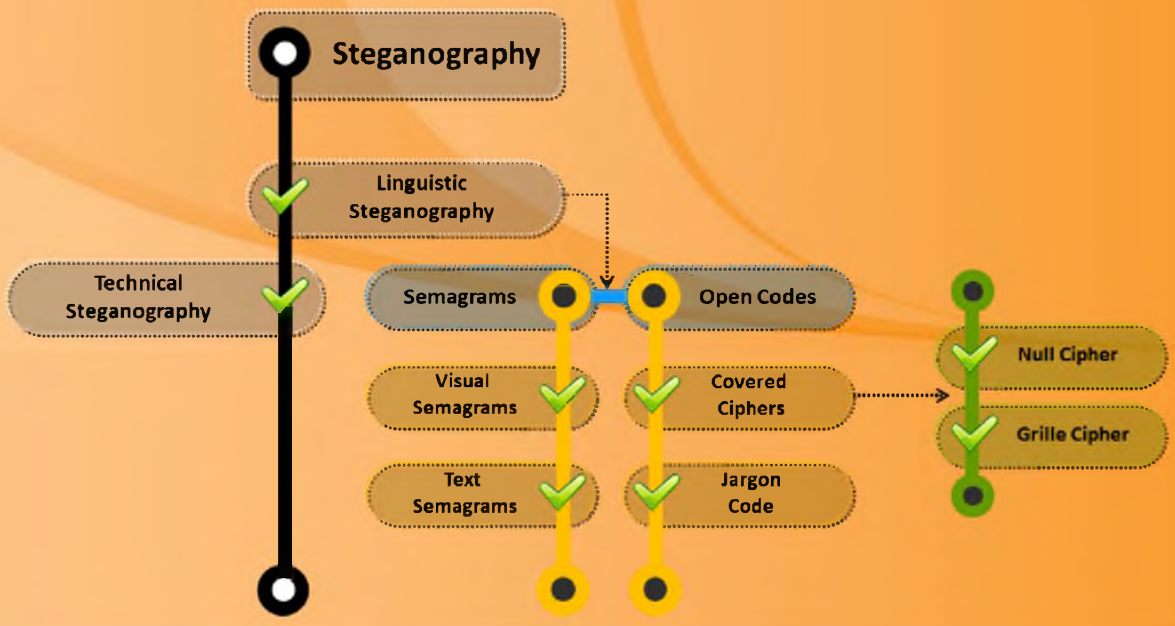
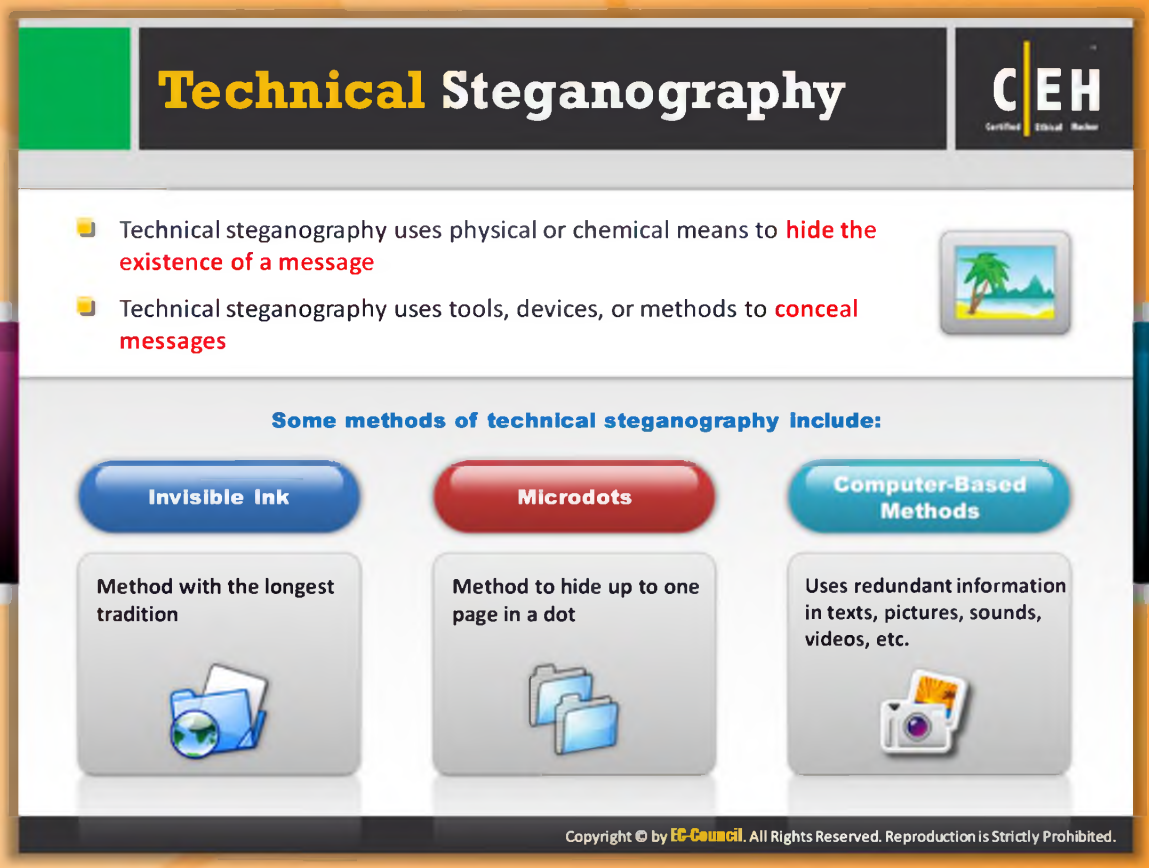


FIGURE 5.64: Classification of Steganography



Technical Steganography

Technical steganography is a method of securing text messages with the help of physical or chemical methods to hide the **existence** of the text message. You can use many tools, devices, and methods.

Technical steganography has methods to **achieve message** hiding. Some of them include:

- **Invisible ink**

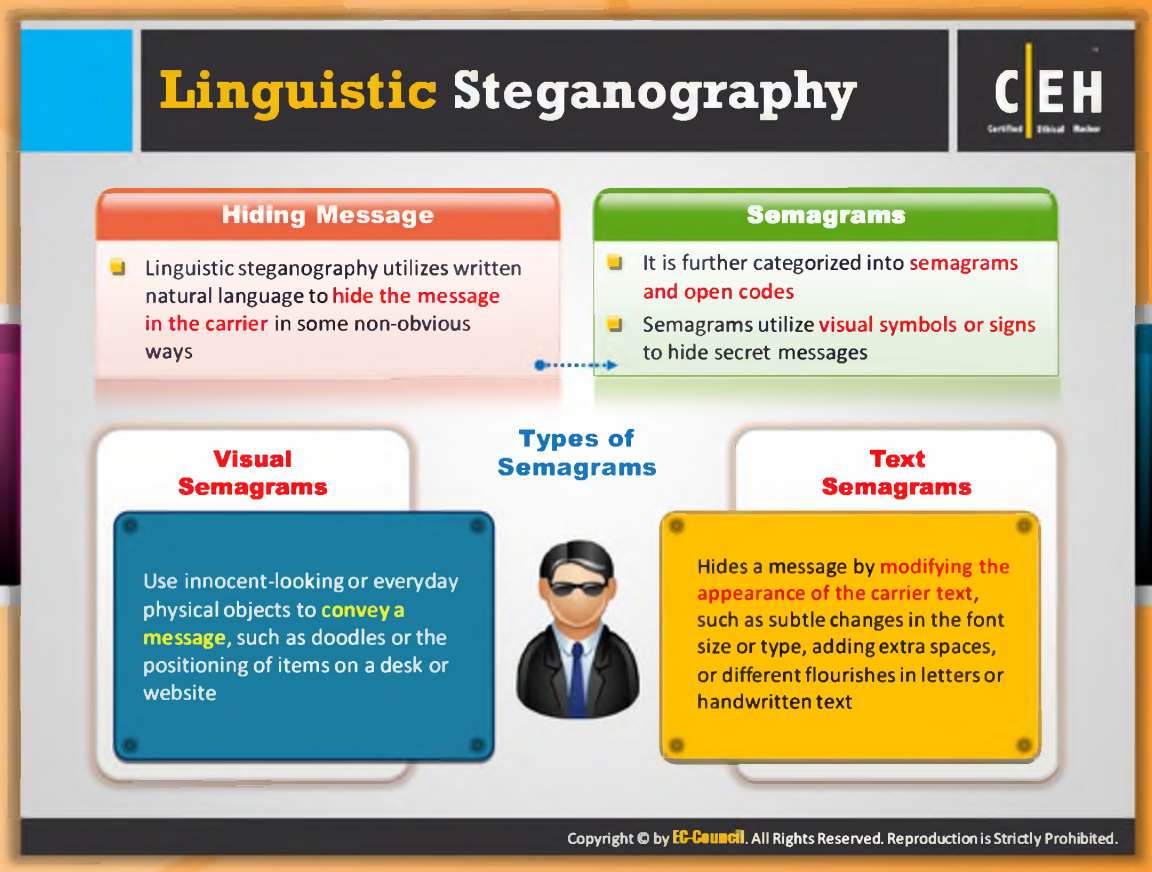
  This method uses invisible ink for hiding text messages.

- **Microdots**

  It is a method that can be used to hide up to one page in a dot.

- **Computer-based methods**

  Use **redundant information** in texts, pictures, sounds, videos, etc.



Linguistic Steganography

Linguistic steganography hides the message in the carrier in some inventive ways. This technique is further categorized as semagrams or open codes.

Semagrams

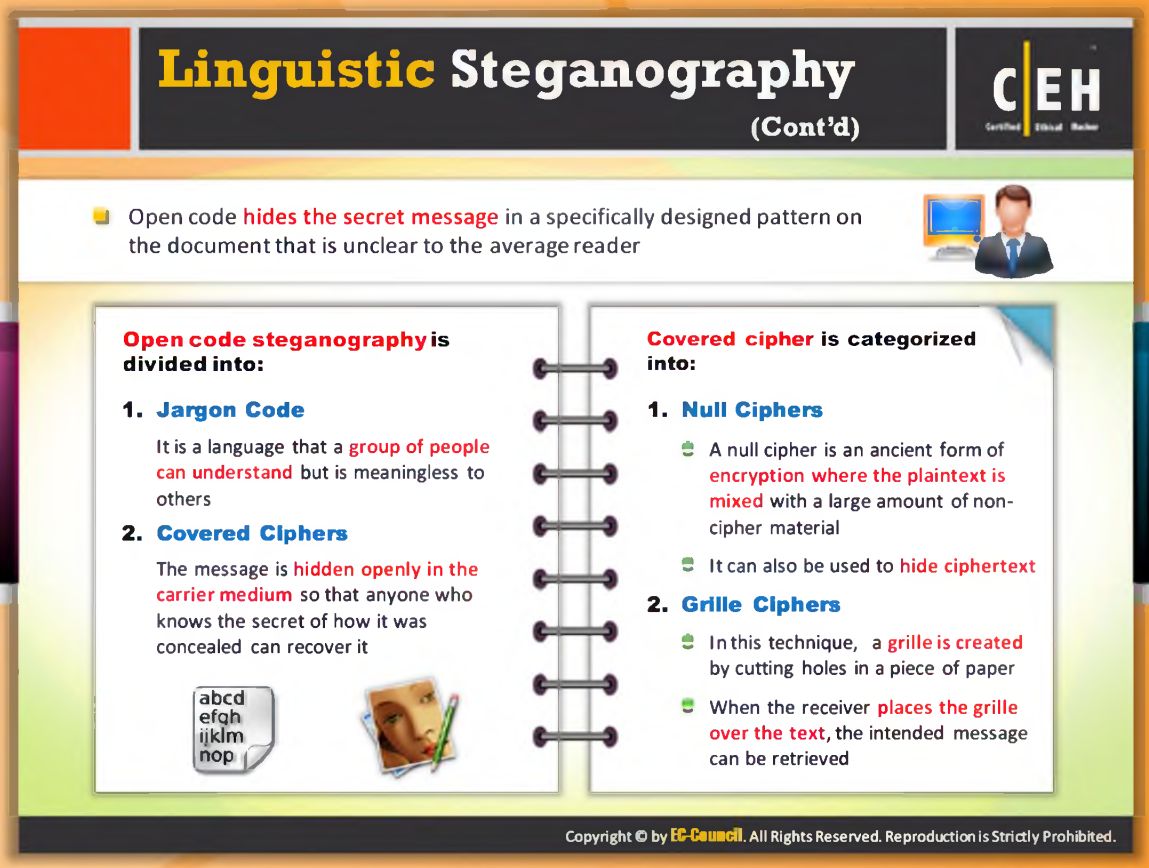
This technique uses symbols and different signs to hide the data or messages. This is further categorized as **visual semagrams** and text semagrams.

- **Visual Semagrams**

  This method uses **unmalicious physical objects** to **transmit** a message such as doodles or the positioning of items on a desk or website.

- **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.



Linguistic Steganography (Cont'd)

Open code hides the secret message in a **legitimate** carrier message that is specifically designed in a pattern on a document that is unclear to the average reader. The carrier message is sometimes called the overt communication and the secret message is the **covert communication**. The open codes technique is divided into two main groups: jargon codes and covered ciphers. The covered ciphers are sub-divided into two types: **null ciphers** and grille ciphers.

Jargon Codes

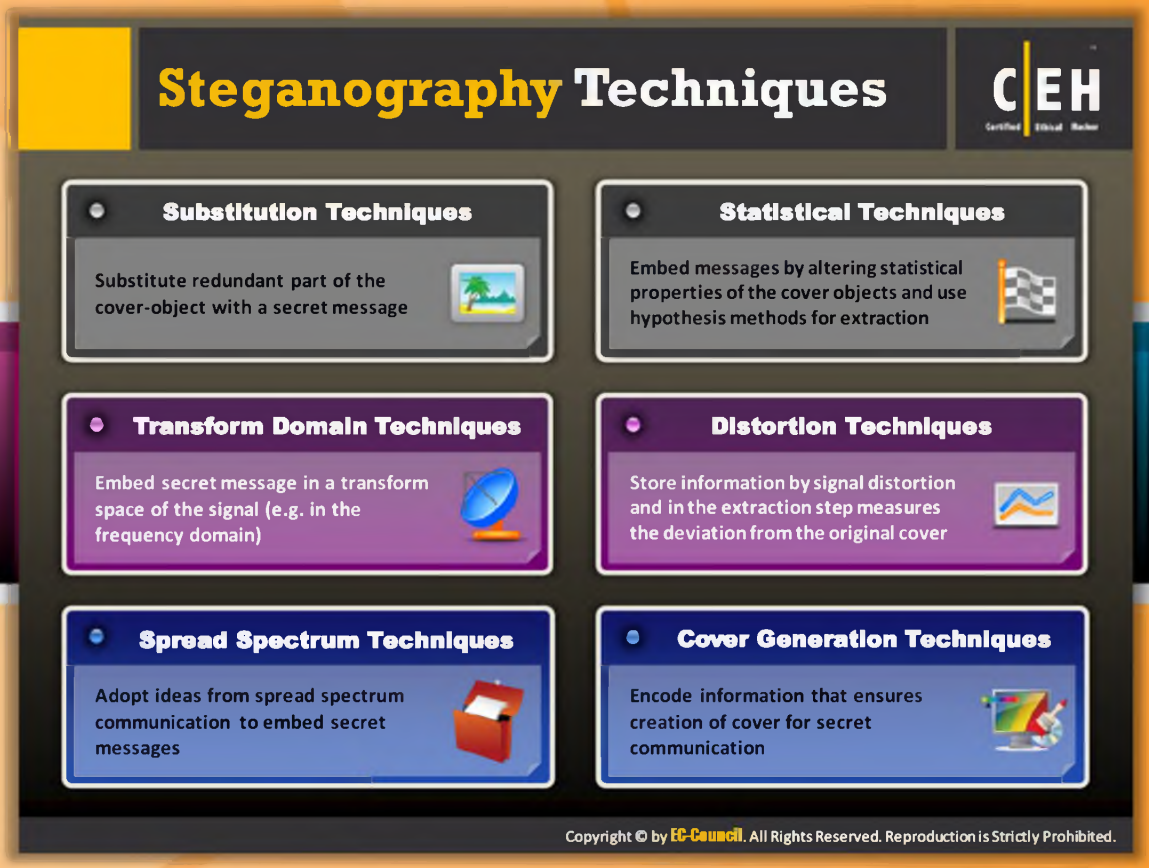
Jargon codes are a language that a group of people can understand but is **meaningless** to others. These codes use signals, terminology, and conversations that have a special meaning that is known to some specific group of people. A subset of jargon codes are cue codes, where certain **prearranged phrases** convey meaning.

Covered Ciphers

The message is hidden openly in the carrier medium so that anyone who knows the secret of how it was **concealed** can recover it. Covered ciphers are **categorized** into two types: **grille ciphers and null ciphers**.

A **grille cipher** employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the **hidden message**.

A **null cipher** hides the message by using some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word." It can also be used to **hide cipher text**.



Steganography Techniques

Steganography techniques are classified into six groups based on 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 secret information is embedded, then they 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. Transformations can be applied to blocks of images or over the entire image.

Spread Spectrum Techniques

This technique provides the means for a low probability of intercept and anti-jamming communications. This is a means of communication in which the signal occupies excess of the

minimum bandwidth to send the information. The excess band spread is accomplished by means of code (independent of data), and a **synchronized** reception with the code is used at the receiver to recover the information from the spread spectrum data.

Statistical Techniques

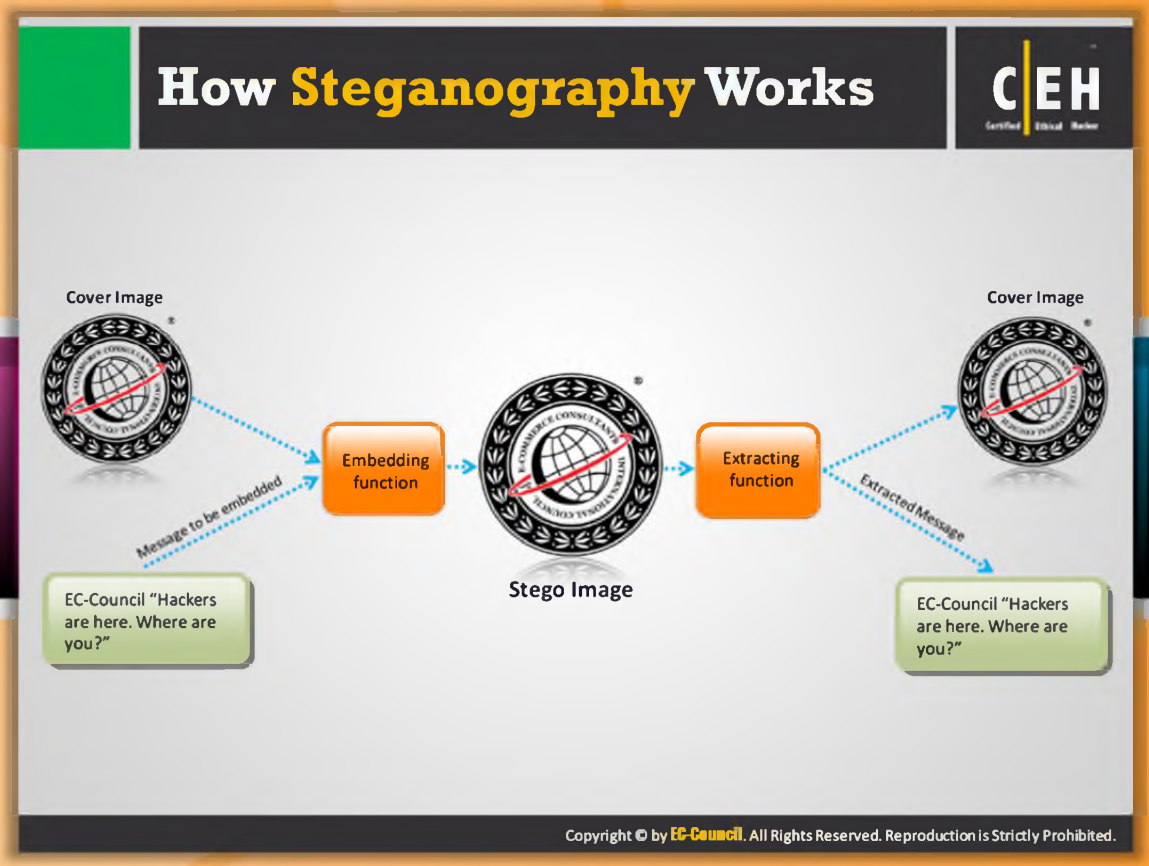
This technique utilizes the existence of "**1-bit**" steganography schemes. This is achieved by modifying the cover in such a way that, when a "1" is transmitted, some of the statistical characteristics change significantly. In other cases the cover remains unchanged. This is done to distinguish between the modified and **unmodified covers**. The theory of hypothesis from mathematical statistics is used for the extraction.

Distortion Techniques

In this technique, a sequence of modifications is applied to the cover in order to get a **stego-object**. The sequence of **modifications** is such that it represents the specific message to be transmitted. 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, digital objects are developed for the purpose of being a cover to **secret communication**. When this information is encoded it ensures the creation of a cover for secret communication.

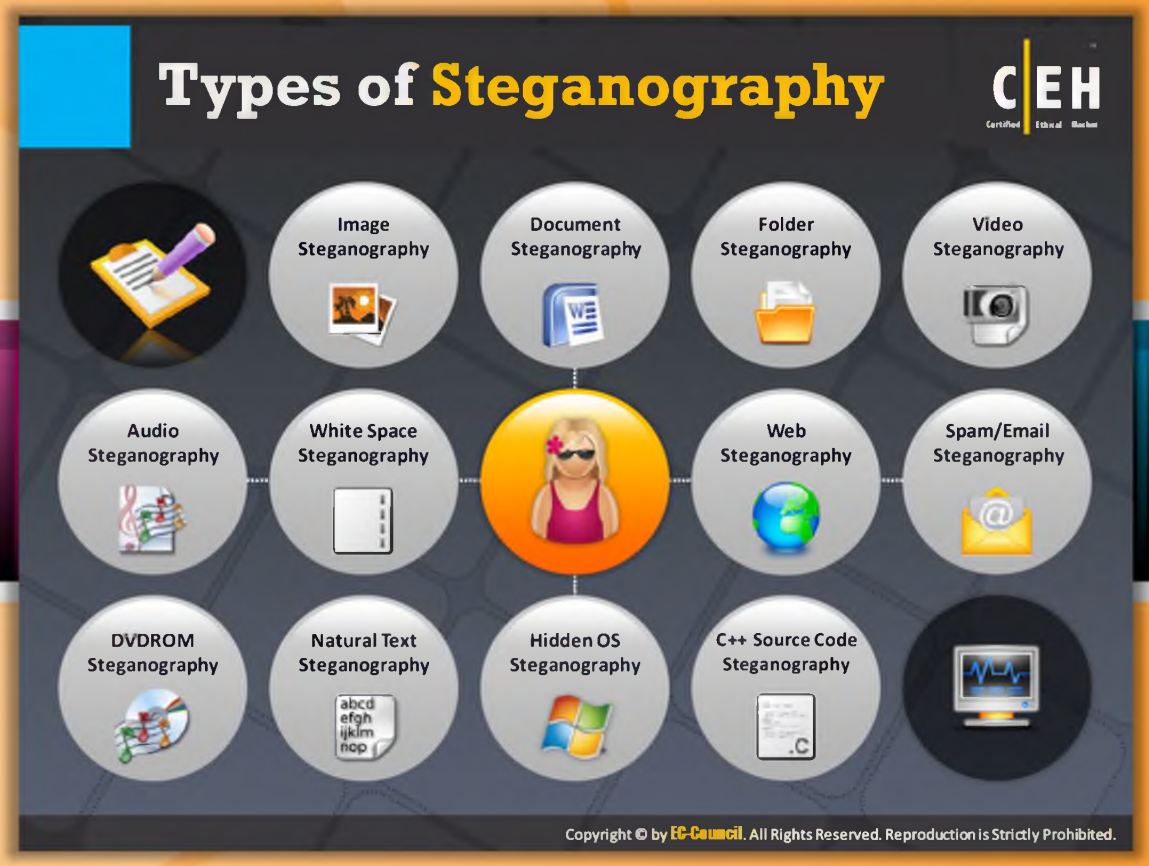


How Steganography Works

Steganography encrypts less important information from digital content and injects hidden data in its place. This is done over image files, text files, audio files, and any digital data. This process is intended to **provide secrecy**. With the introduction of the Internet, hidden messages inside digital images became the most common and highly effective form of steganography. Images are stored in the computer as a group of **pixels**, with one pixel being around 8 to 24 bits. This group of pixels is stored in an image file according to any one of a number of formats. There are two files that are needed to hide a message within an image file. They are:

1. The file containing the image into which the message is supposed to be put
2. The file containing the message itself

FIGURE 5.65: How Steganography Works



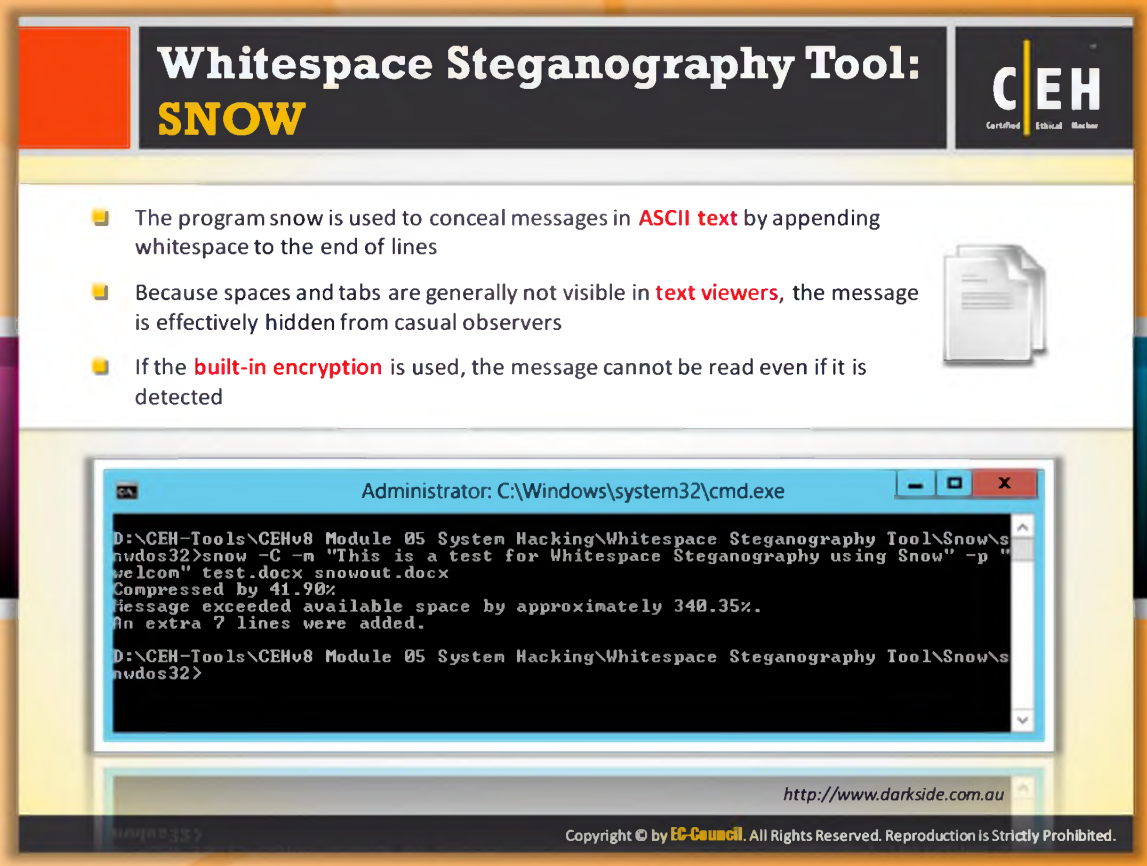
Types of Steganography

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 divided into **watermarking and fingerprinting**.

The different types of steganography are listed as follows:

- Image Steganography
- Document steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- Whitespace Steganography
- Web Steganography

- Spam/Email Steganography
- DVDROM Steganography
- Natural Text Steganography
- Hidden OS Steganography
- C++ Source Code Steganography



Whitespace Steganography Tool: SNOW

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

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

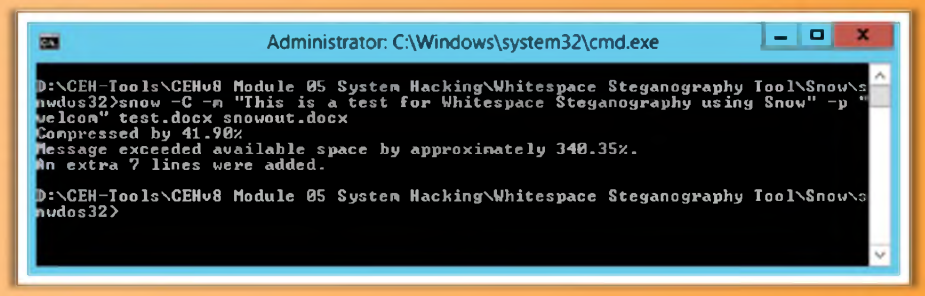


FIGURE 5.66: Whitespace Steganography Tool by Using SNOW

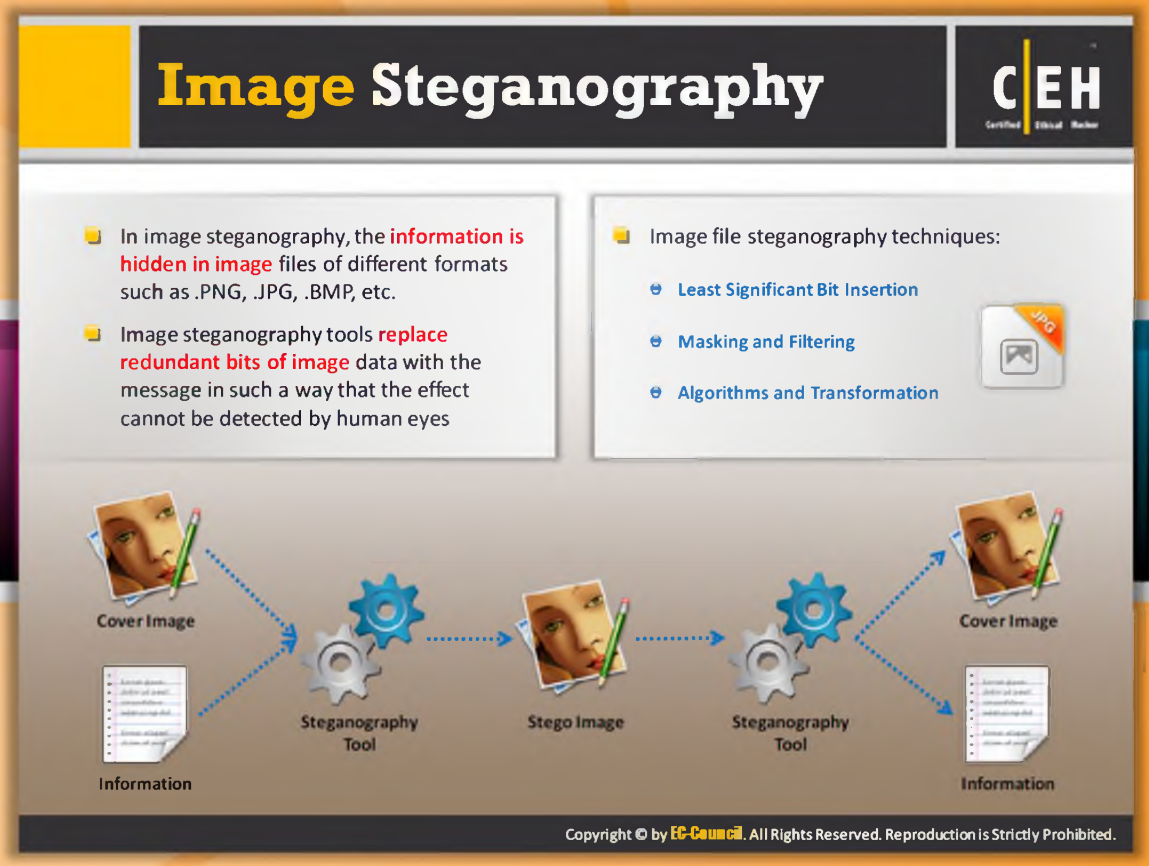


Image Steganography

Image steganography allows you to conceal your secret message within an image. You can take **advantage** of the **redundant bit** of the image to conceal your message within it. These redundant bits are those bits of the image that have very little effect on the image if altered. This **alteration** of bits is not detected easily. You can conceal your information within images of different formats such as .PNG, .JPG, .BMP, etc.

Images are the popular cover objects used for steganography. Image steganography tools are used to replace **redundant bits** of image data with the message in such a way that the effect cannot be detected by human eyes.

Image steganography techniques can be divided into two groups: Image domain and transform domain. In image (spatial) **domain techniques**, messages are embedded in the intensity of the pixels directly. In transform domain (frequency) techniques, images are first **transformed** and then the message is embedded in the image.

There are three techniques that you can use to conceal you **secret messages** in image files:

- Least Significant Bit Insertion
- Masking and Filtering
- **Algorithms** and **Transformation**

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

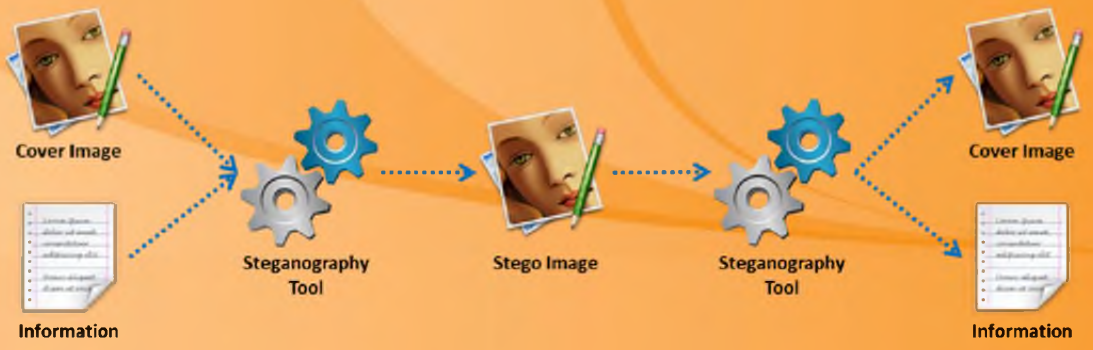
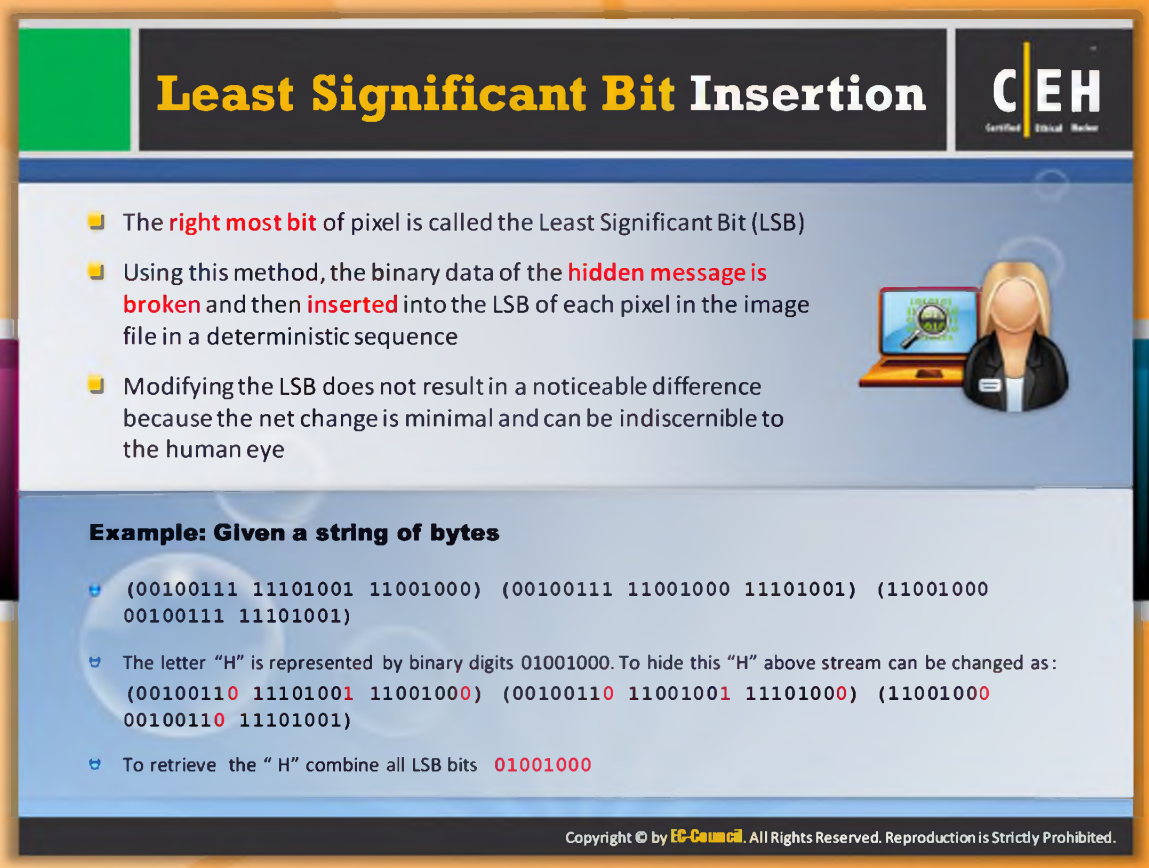


FIGURE 5.67: How Image Steganography Works



Least Significant Bit Insertion

The Least Significant Bit **Insertion** technique is the most commonly used technique of image steganography in which the Least Significant Bit (LSB) of each pixel is used to hold your secret data. The LSB is the **rightmost** bit of each pixel of image file. This LSB, if changed, has very little effect on the image; it cannot be **detected**. To hide the message, first break the message and insert each bit in place of each pixel's LSB of the image so that the recipient at the other end can retrieve your message easily.

Suppose you have chosen a 24-bit image to hide your **secret data**, which can be represented 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 as follows.

Now letter "H" is represented by binary digits 01001000. To hide this "H," the previous stream can be changed to:

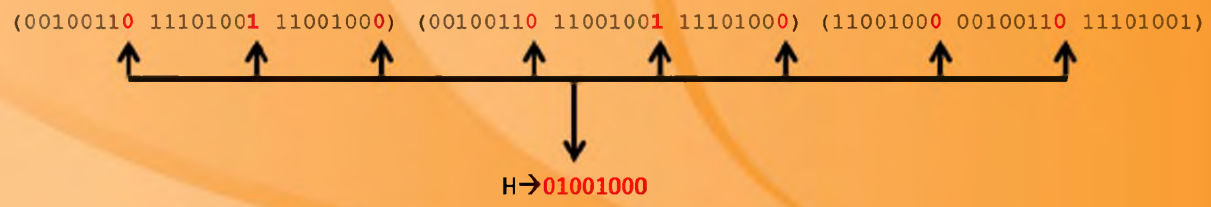
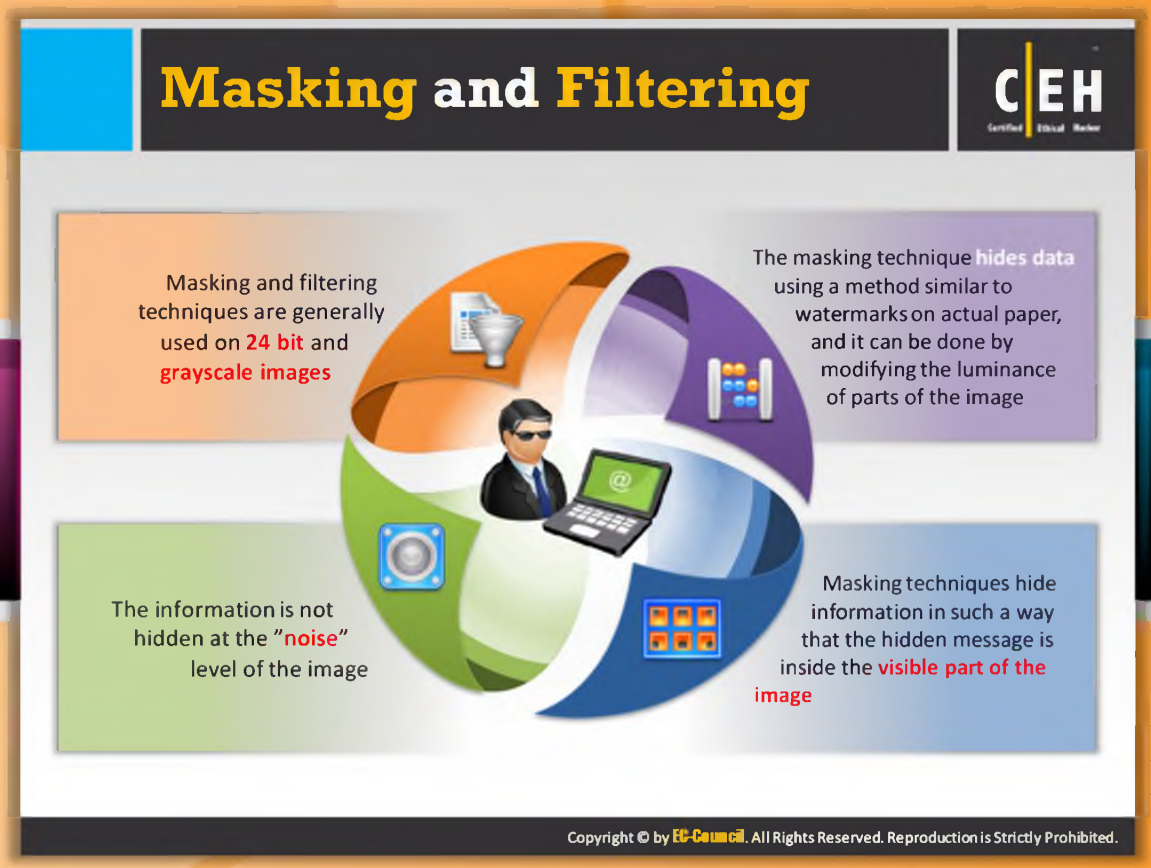


FIGURE 5.68: Least Significant Bit Insertion Diagram

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

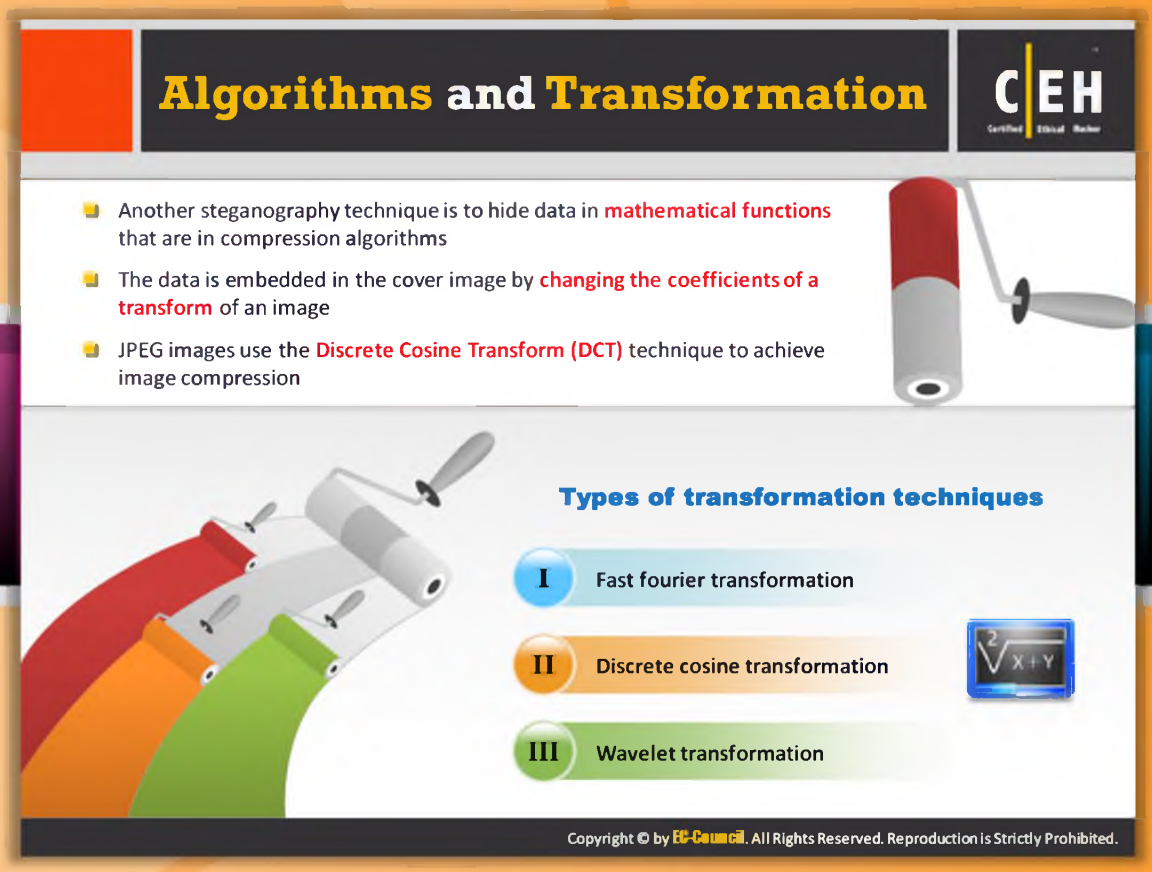
To retrieve this H at the other side, the person at the **receiver side** combines all the **LSB bits** of the image file and thus is able to detect the H at the receiver side.



Masking and Filtering

Masking and filtering techniques take advantage of human visual capabilities that cannot detect the slight changes in particular images. **Grayscale images** can hide information in a way that is similar to watermarks on paper and are sometimes used as digital watermarks.

The masking technique allows you to conceal your secret data by placing it on an images file. Both masking and **filtering techniques** are mostly used on **24-bit-per-pixel images** and grayscale images. To hide secret messages, you need to adjust the luminosity and opacity of the image. If the change in the luminance is small, then people other than the intended users fail to notice that the image contains a **hidden message**. This technique can be easily applied to the image as it does not disturb the image. it is mostly used with **JPEG images**. Lossy JPEG images are relatively immune to cropping and compression image operations. Hence, the information is hidden in **lossy JPEG** images often using the masking technique. The reason that a **steganography image** encoded with a marking **degrades** in a lower rate under JPEG compression is that the message is hidden in the **significant** areas of the picture.



Algorithms and Transformation

The **algorithms** and **transformation technique** is based on hiding the secret information during the compression of the image.

In this technique, the information on the image is concealed by applying various compression algorithms and transformation functions. **Compression algorithm** and transformation uses a **mathematical function** to hide the coefficient of least bit during compression of images. Generally JPEG images are suitable to perform **compression** as they can be saved at different compression levels. This technique gives you high **level of invisibility** of secret data. JPEG images use a discrete cosine transform to achieve compression.

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

- Fast fourier transformation
- **Discrete cosine** transformation
- Wavelet transformation

Image Steganography: QuickStego

Source: http://quickcrypto.com

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

QuickStego **imperceptibly** alters the pixels (individual picture elements) of the image, encoding the secret text by adding small variations in color to the image. In practice, to the human eye, these small differences do not appear to change the **image**.

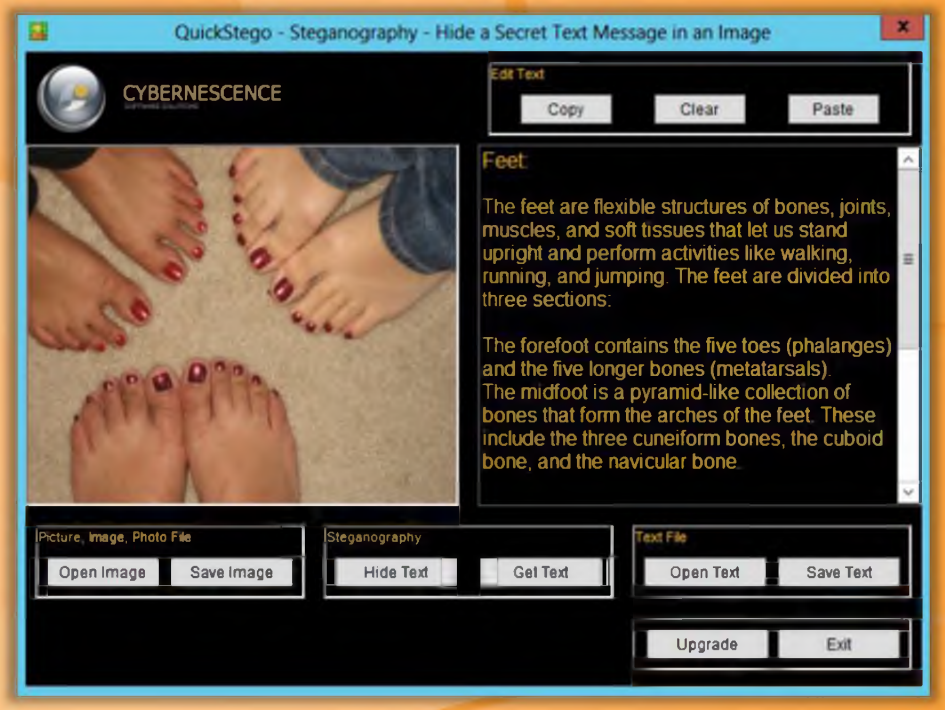


FIGURE 5.69: QuickStego Screenshot

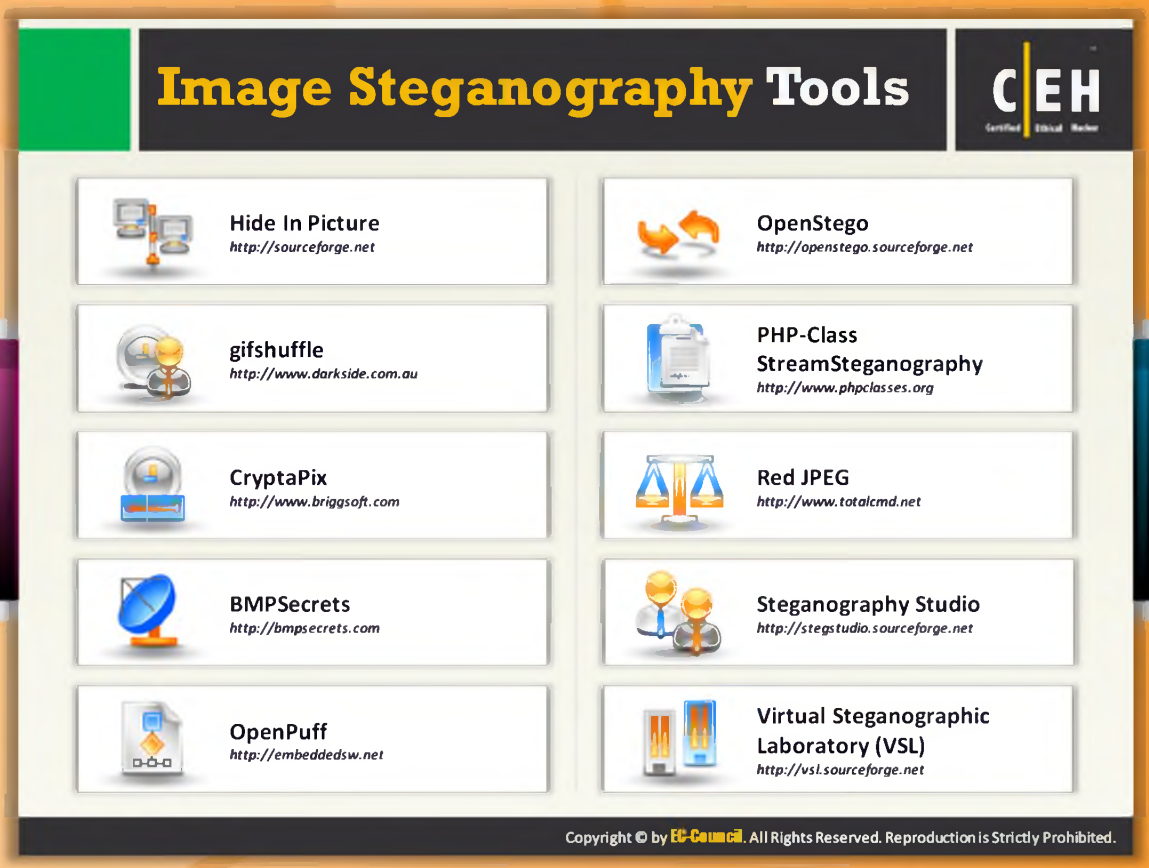
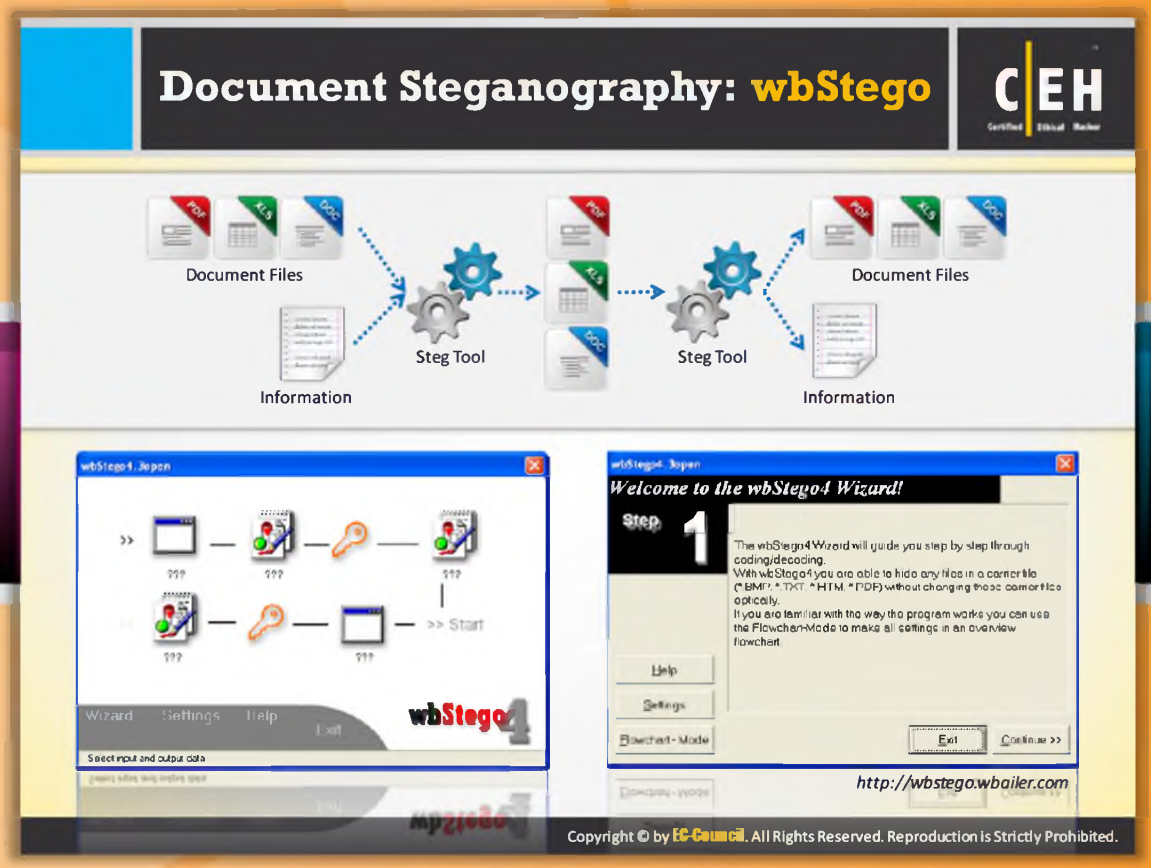


Image Steganography Tools

Like the tool **QuickStego** discussed previously, you can also use the following image steganography tools to hide your secret messages in images:

- Hide In Picture available at http://sourceforge.net
- gifshuffle available at http://www.darkside.com.au
- CryptaPix available at http://www.briggsoft.com
- BMPSecrets available at http://bmpsecrets.com
- OpenPuff available at http://embeddedsw.net
- OpenStego available at http://openstego.sourceforge.net
- PHP-Class StreamSteganography available at http://www.phpclasses.org
- Red JPEG available at http://www.totalcmd.net
- Steganography Studio available at http://stegstudio.sourceforge.net
- Virtual Steganographic Laboratory (VSL) available at http://vsl.sourceforge.net



Document Steganography

Similar to image steganography, document steganography is the **technique** used to **hide secret messages** to be transferred in documents. The following diagram illustrates the document steganography process:

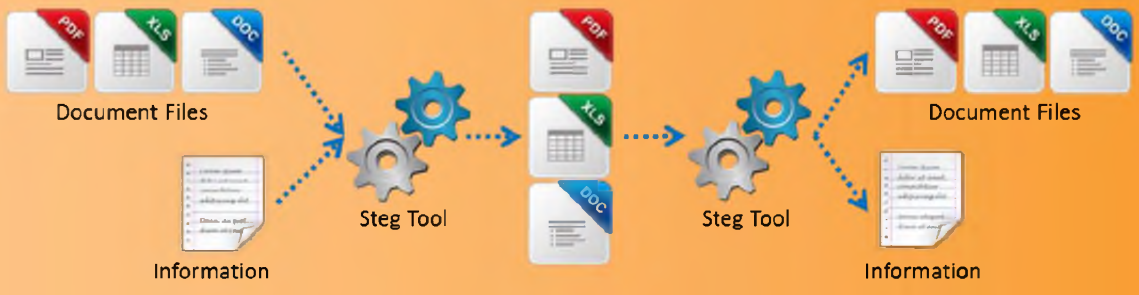


FIGURE 5.70: Working of Document Steganography

Document Steganography: 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**.

FIGURE 5.71: wbStego Screenshot

Document Steganography Tools

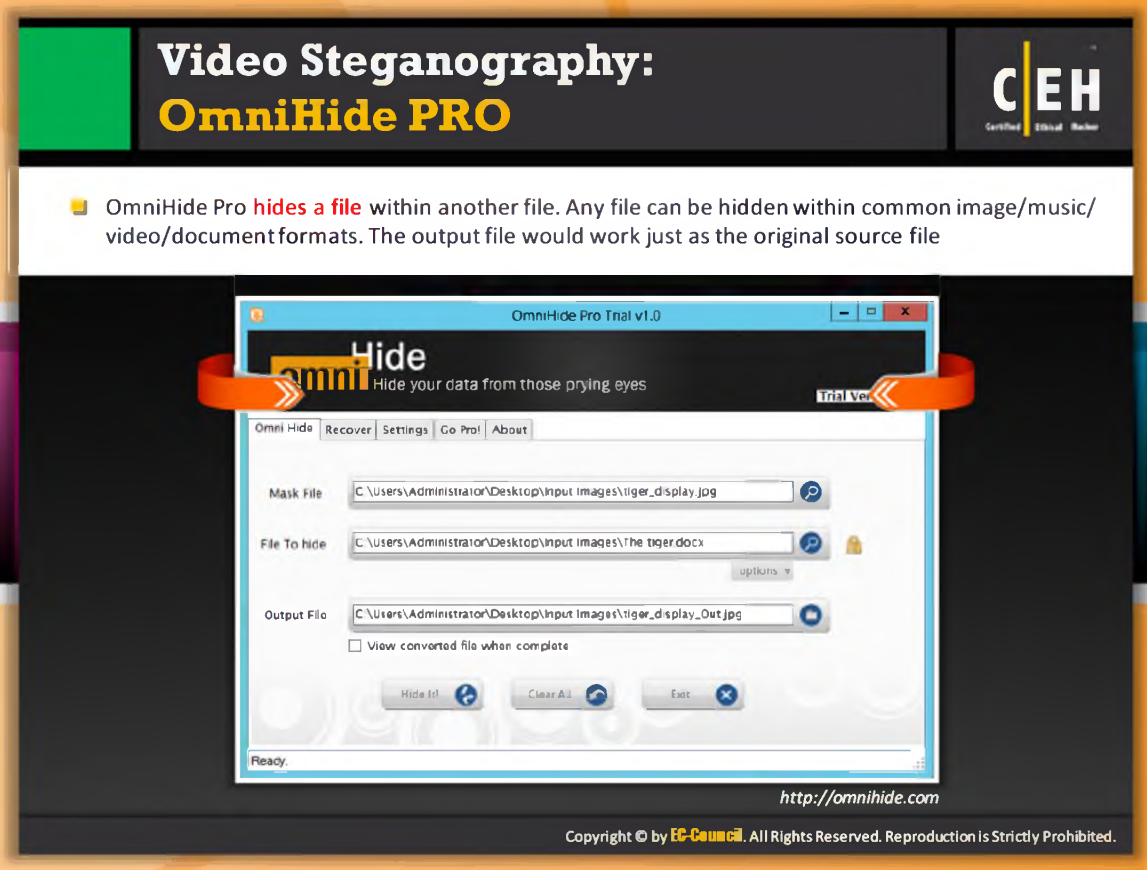
Similar to **wbStego**, there are many other tools that allow you to hide data within other document files of various types or **extension**:

- Merge Streams available at http://www.ntkernel.com
- Office XML available at http://www.irongeek.com
- Data Stash available at http://www.skyjuicesoftware.com
- FoxHole available at http://foxhole.sourceforge.net
- Xidie Security Suite available at http://www.stegano.ro
- StegParty available at http://www.fasterlight.com
- Hydan available at http://www.crazyboy.com
- StegJ available at http://stegj.sourceforge.net
- StegoStick available at http://sourceforge.net
- SNOW available at http://www.darkside.com.au

Video Steganography

Video steganography involves **hiding secret messages** files of any extensions in the continuously flowing video file. Here video files are used 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 continuous flow of the video.

As a video file is a combination of image and audio, all the techniques available for image and audio steganography can also be applied to **video steganography**. It can be used to hide a large number of **secret messages**.



Video Steganography: OmniHide PRO

Source: http://omnihide.com

OmniHide PRO allows you to hide any secret file within **innocuous image**, video, music files, etc. The resultant **Stego file** can be used or shared like a normal file without anyone knowing that something is hidden within it, 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:

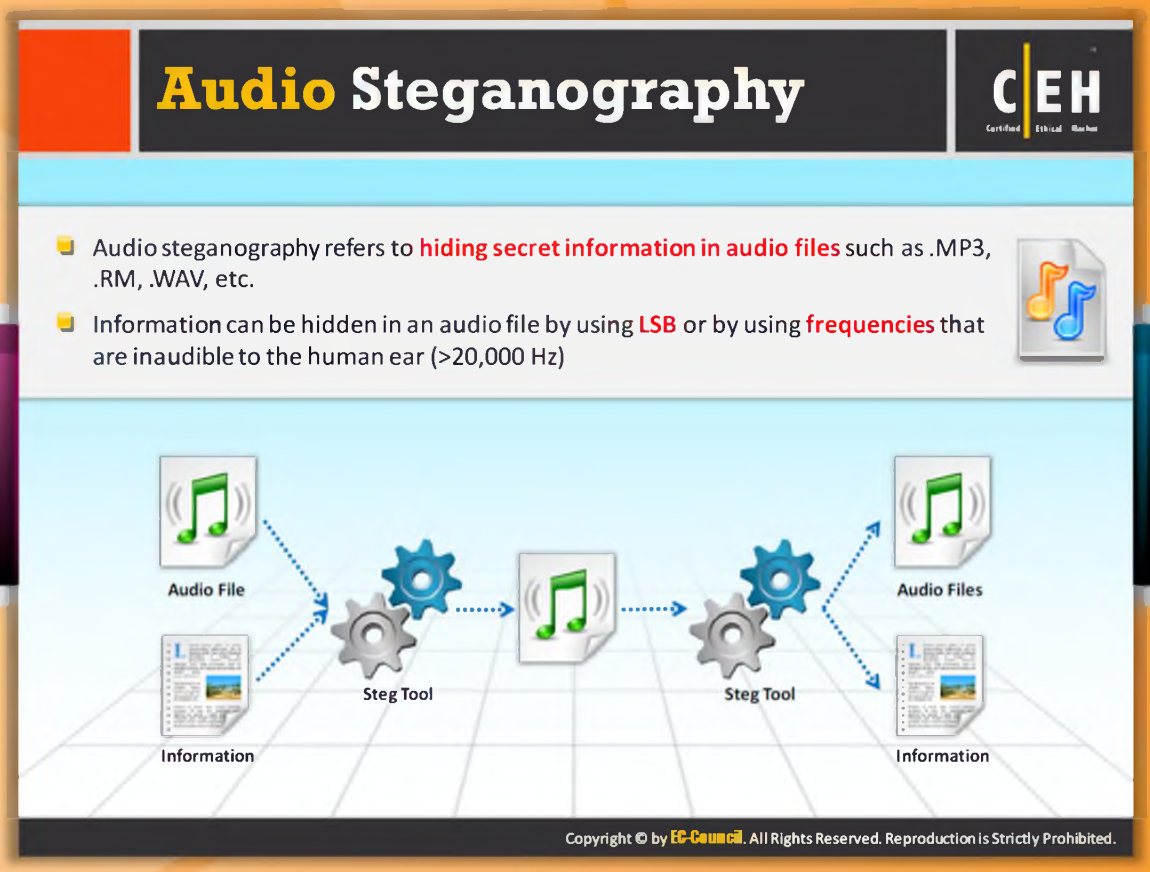
- This allows you to hide you files in Photos, Movies, Documents, and Music etc.
- It put no **limitation** on file type and size you want to hide

FIGURE 5.72: OmniHide PRO Screenshot

Video Steganography Tools

In addition to **PRO**, there are many other tools that you can use to hide your secret information file in video files:

- Our Secret available at http://www.securekit.net
- RT Steganography available at http://rtstegvideo.sourceforge.net
- Masker available at http://www.softpuls.com
- Max File Encryption available at http://www.softeza.com
- MSU StegoVideo available at http://www.compression.ru
- BDV DataHider available at http://www.bdvnotepad.com
- StegoStick available at http://sourceforge.net
- OpenPuff available at http://embeddedsw.net
- Stegsecret available at http://stegsecret.sourceforge.net
- PSM Encryptor available at http://demo.powersoftmakers.com

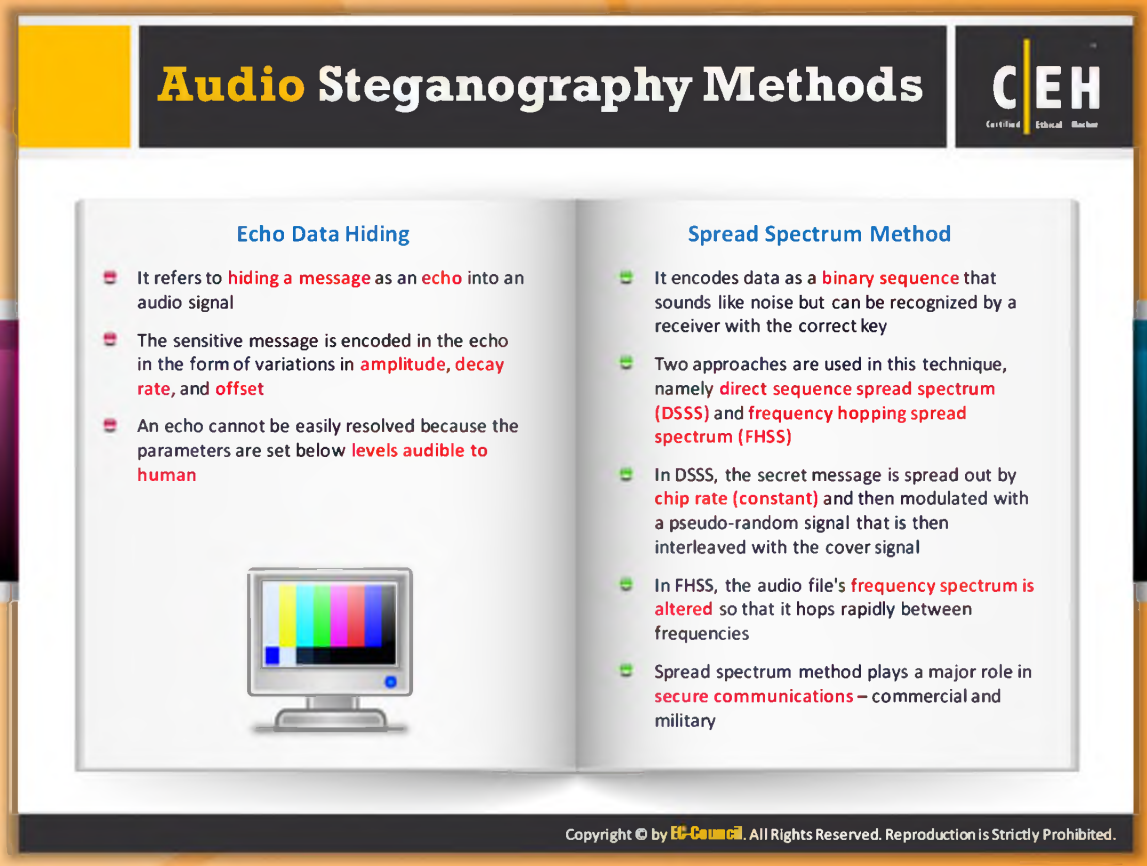


Audio Steganography

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

You need to ensure that the carrier audio file should not be significantly degraded due to embedded secret data; otherwise, the **eavesdropper** can detect the existence of the hidden message in the audio file. So the secret data should be embedded in such a way that there is a slight change in the audio file that cannot be detected by a human. Information can be hidden in an audio file by using an **LSB** or by using frequencies that are **inaudible** to the human ear (>20,000 Hz).

FIGURE 5.73: Working of Audio Steganography



Audio Steganography Methods

There are certain methods available to conceal your secret messages in **audio files**. Some methods implement the algorithm that is based 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 are used to perform audio **steganography** in order to hide secret information.

Echo Data Hiding

In the echo data **hiding method**, the secret **information is embedded** within 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, these two signals get mixed at a certain point of time where it is not possible for the human ear to distinguish between these two signal. At this point, an echo sound can be heard as an added resonance to the original signal. However, this point of **undistinguishable** sounds depends on factors such as quality of **original audio signal**, type of sound, and listener.

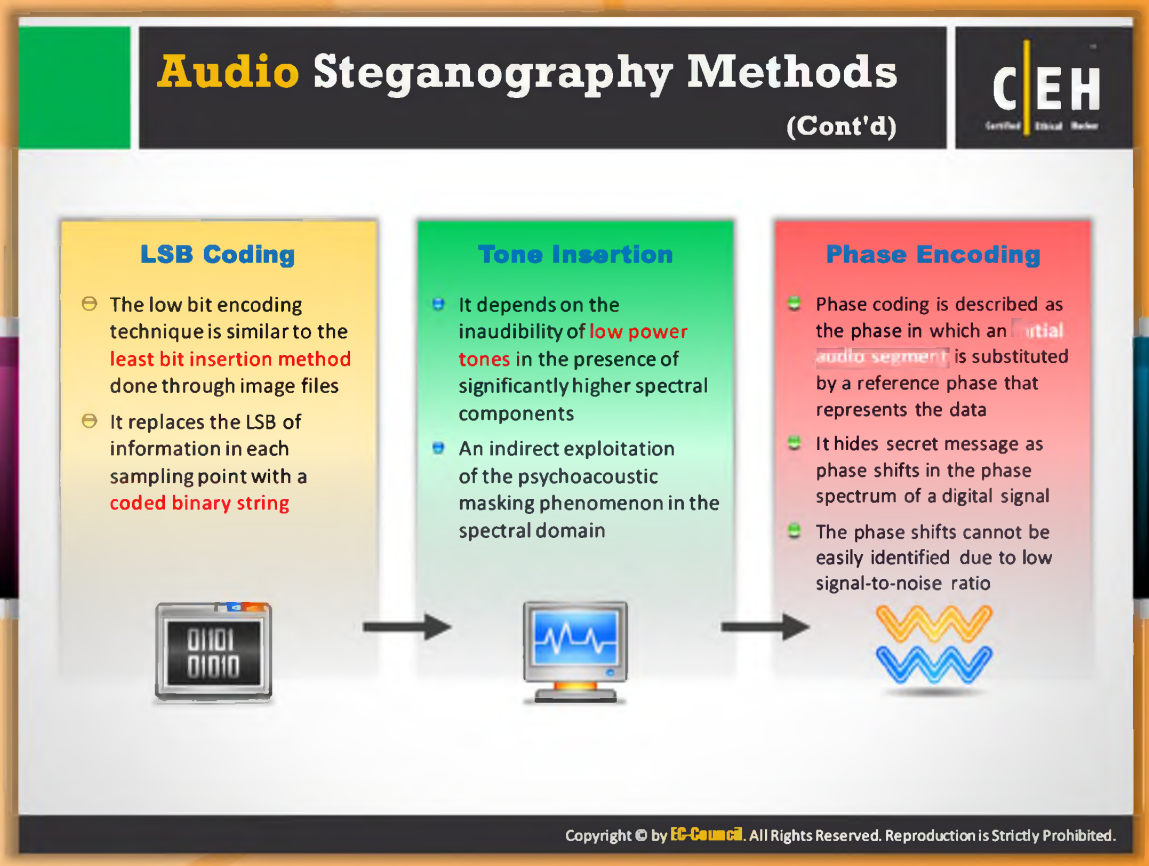
To encode the resultant signal in to binary form, two different delay times are used. These delay times should be below **human perception**. Parameters such as decay rate and initial amplitude should also be set below threshold audible values so that the audio is not **hearable** at all.

Spread Spectrum Method

In this method, secret information is spread across as much of the frequency spectrum as possible. This method uses two versions of spread spectrum viz.: **direct sequence spread spectrum (DSSS)** and frequency hopping spread spectrum (FHSS)

In **DSSS**, the secret message is spread out by **chip rate** (constant) and then modulated with a pseudo-random signal that is then **interleaved** with the cover signal.

In **FHSS**, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies. Spread spectrum method plays a major role in secure communications, both commercial and military.



Audio Steganography Methods (Cont'd)

LSB Coding

LSB encoding works like the LSB insertion technique in which a secret binary message is inserted in the least significant bit of each sampling point of the audio signal. This method can be used to hide large amounts of secret data. It is possible to use the last two significant bits to insert secret binary data but the problem is that it will create noise in the audio file. Its poor immunity to manipulation makes this method less adaptive. Hidden data can be easily identified and extracted due to channel noise and resampling.

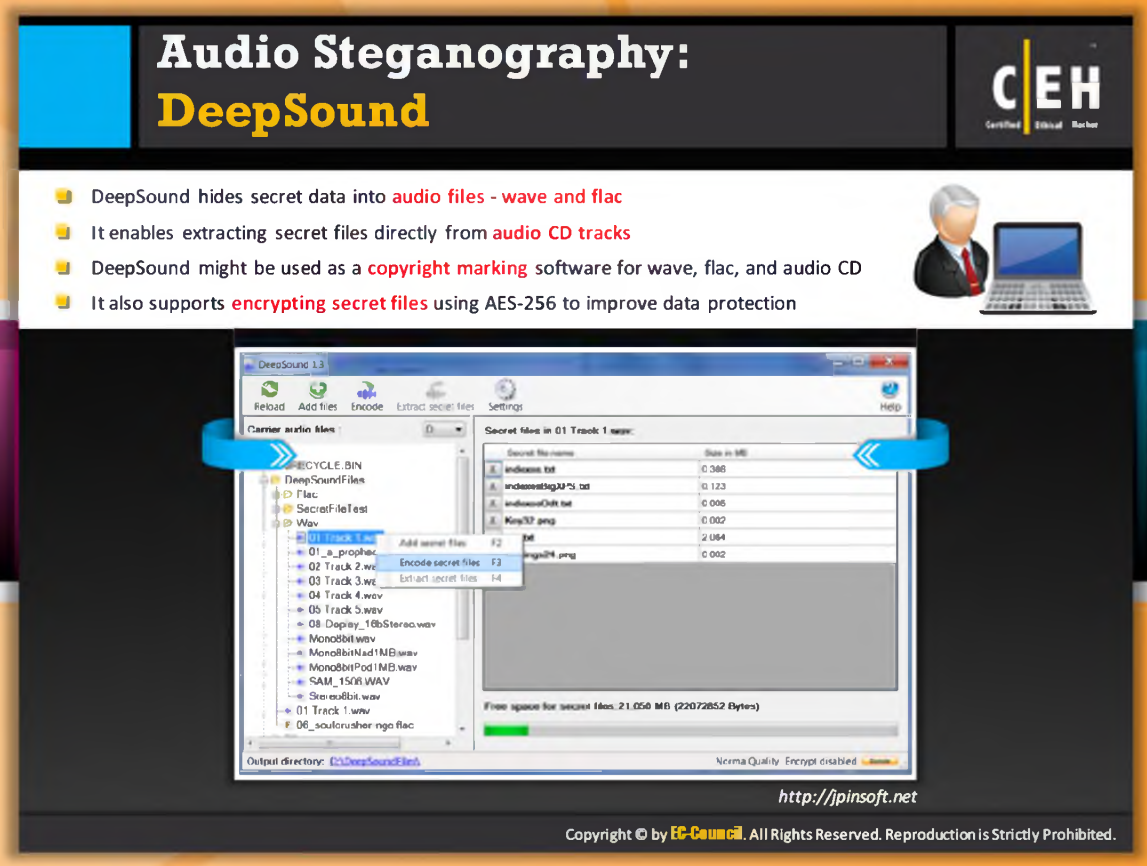
Tone Insertion

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.



Audio Steganography: DeepSound

Source: http://jpinsoft.net

DeepSound helps you to hide any kind of secret data into 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. It also 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).

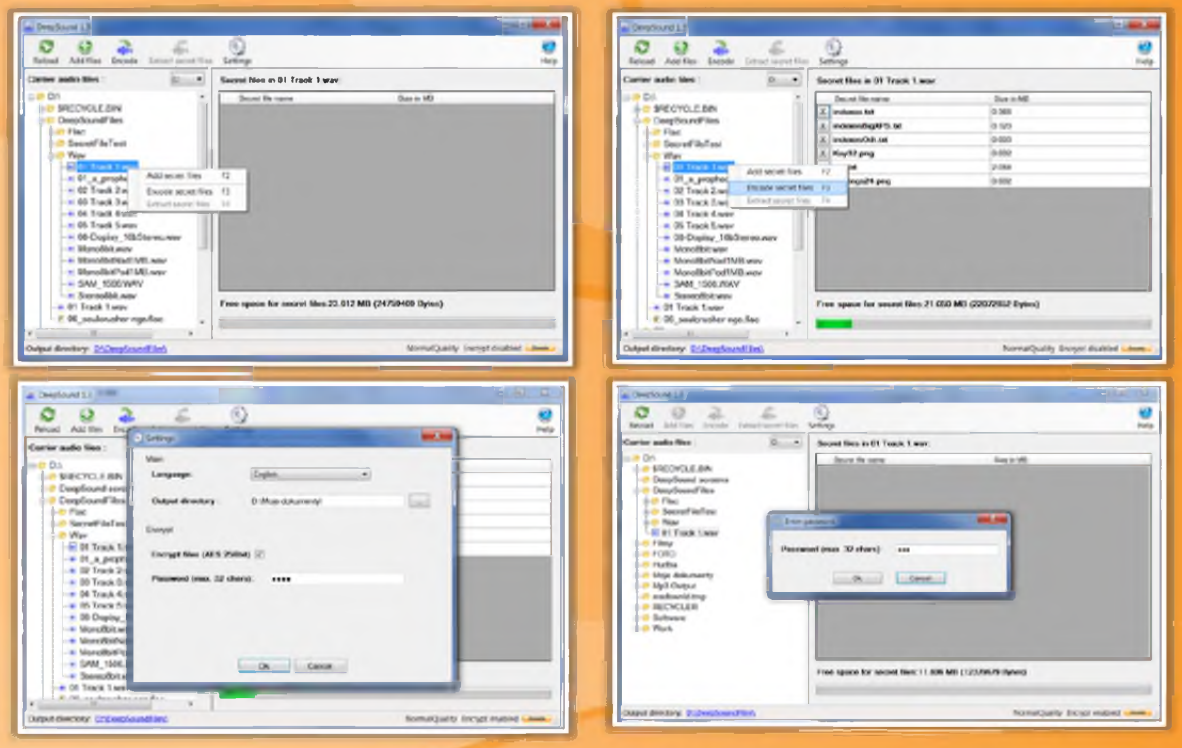
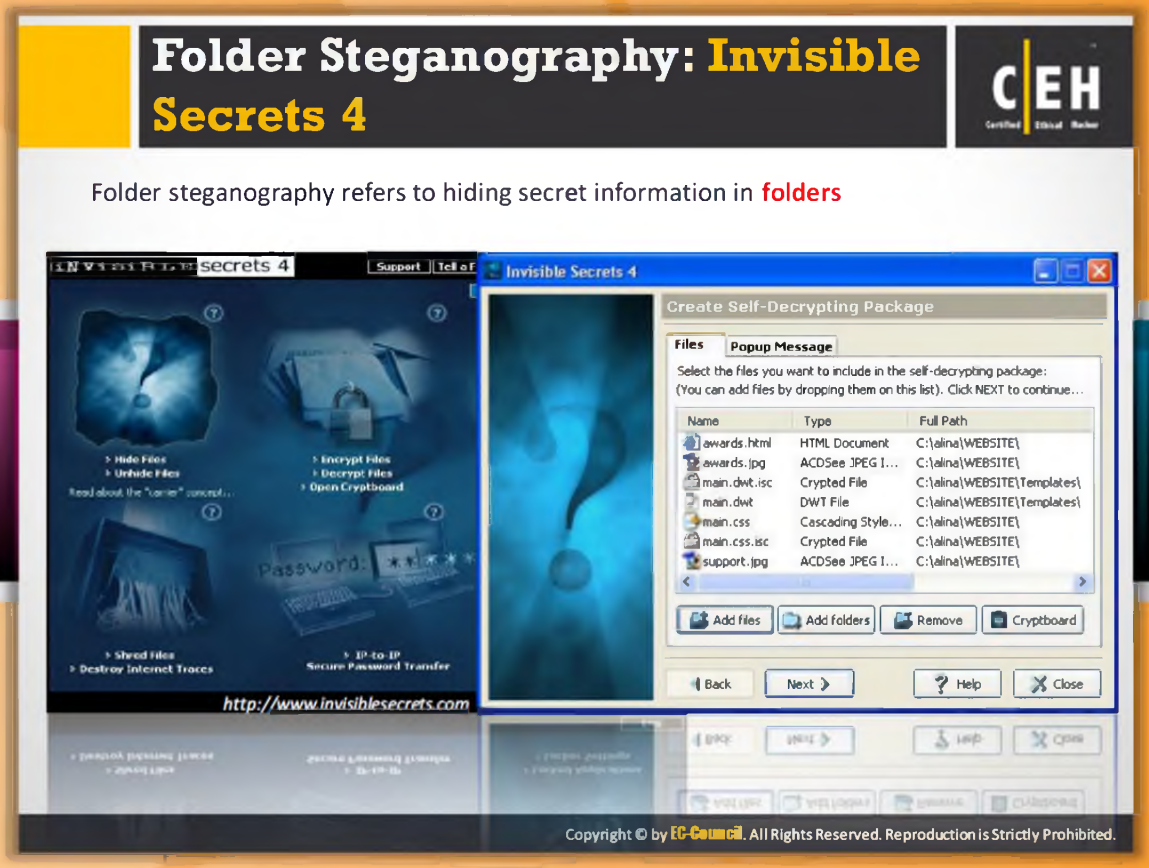


FIGURE 5.74: DeepSound Screenshot

Audio Steganography Tools

You can also use the following audio **steganography tools** to hide your secret information in audio files:

- Mp3stegz available at http://sourceforge.net
- MAXA Security Tools available at http://www.maxa-tools.com
- BitCrypt available at http://bitcrypt.moshe-szweizer.com
- MP3Stego available at http://www.petitcolas.net
- Hide4PGP available at http://www.heinz-repp.onlinehome.de
- CHAOS Universal available at http://safechaos.com
- SilentEye available at http://www.silenteye.org
- QuickCrypto available at http://www.quickcrypto.com
- CryptArkan available at http://www.kuskov.com
- StegoStick available at http://sourceforge.net



Folder Steganography: Invisible Secrets 4

Folder steganography refers to **hiding secret** information in folders. This can be accomplished with the help of the tool Invisible Secrets 4.

Source: http://www.invisiblesecrets.com

Invisible Secrets 4 is file **encryption software** that keeps **cybercriminals** out of your emails and prevents attackers from viewing your private files. This software not only encrypts your private data and files for safe keeping and **securing transfer** across the net, but also hides them in such a place that no one can identify them. Even an attacker could not locate **sensitive information**. Since the places the private documents are kept appear totally innocent, such as picture or sound files or web pages, these types of files are a perfect **disguise** for 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**.

FIGURE 5.75: Invisible Secret Autorun

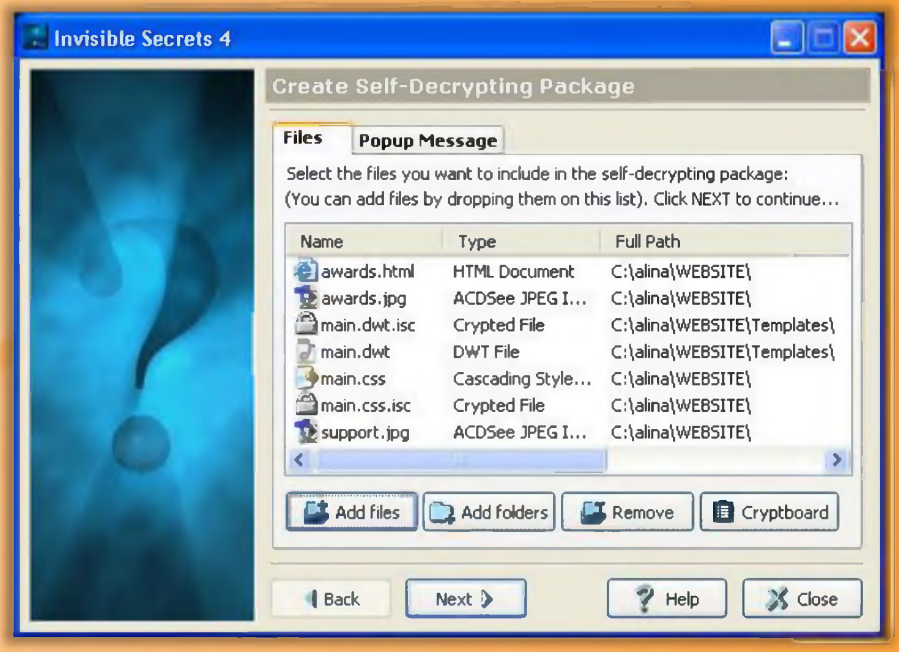


FIGURE 5.76: Invisible Secret Screenshot

Folder Steganography Tools

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

- Folder Lock available at http://www.newsoftwares.net
- A+ Folder Locker available at http://www.giantmatrix.com
- Toolwiz BSafe available at http://www.toolwiz.com
- Hide Folders 2012 available at http://fspro.net
- GiliSoft File Lock Pro available at http://www.gilisoft.com
- Universal Shield available at http://www.everstrike.com
- WinMend Folder Hidden available at http://www.winmend.com
- Encrypted Magic Folders available at http://www.pc-magic.com
- QuickCrypto available at http://www.quickcrypto.com
- Max Folder Secure available at http://www.maxfoldersecure.com

Spam/Email Steganography: Spam Mimic

Spam/email steganography refers to the technique of sending secret messages by hiding them in spam/email messages. Spam emails can be used as the way of secret communication by embedding the secret messages in some way and hiding the embedded data in the spam emails. This technique is supposedly to be used by various military agencies, with the help of steganographic algorithms. This can be accomplished with the help of the Spam Mimic tool.

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.

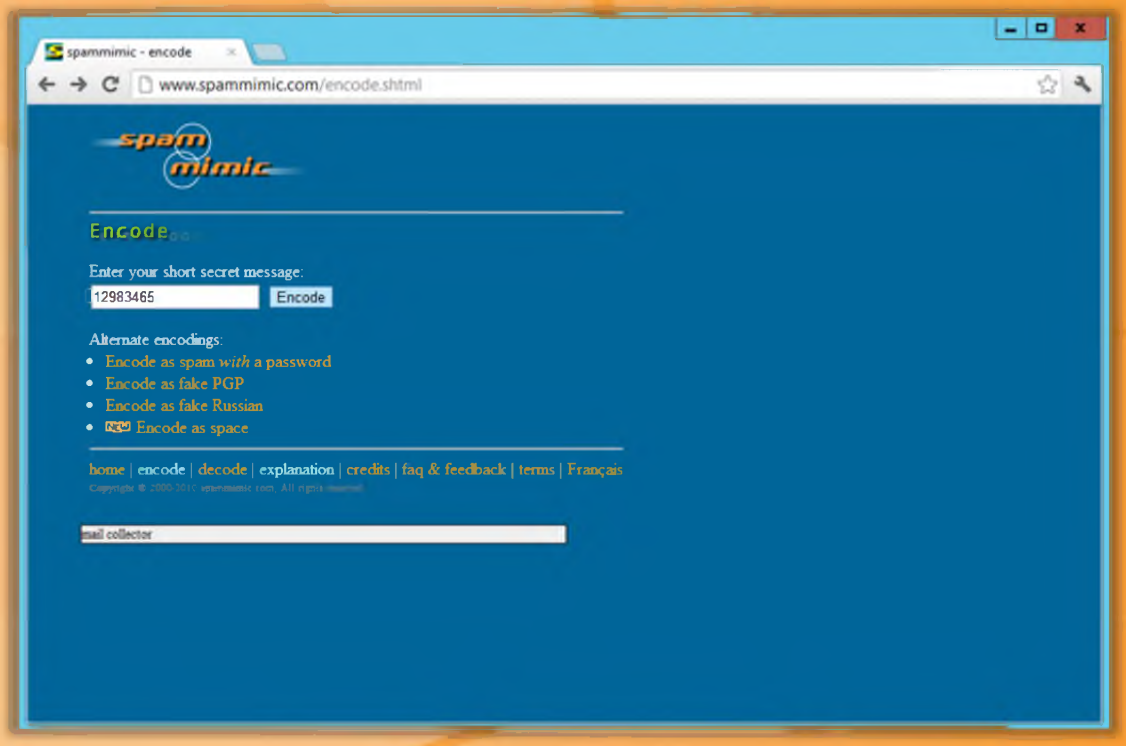


FIGURE 5.77: Spam Mimic Login Page

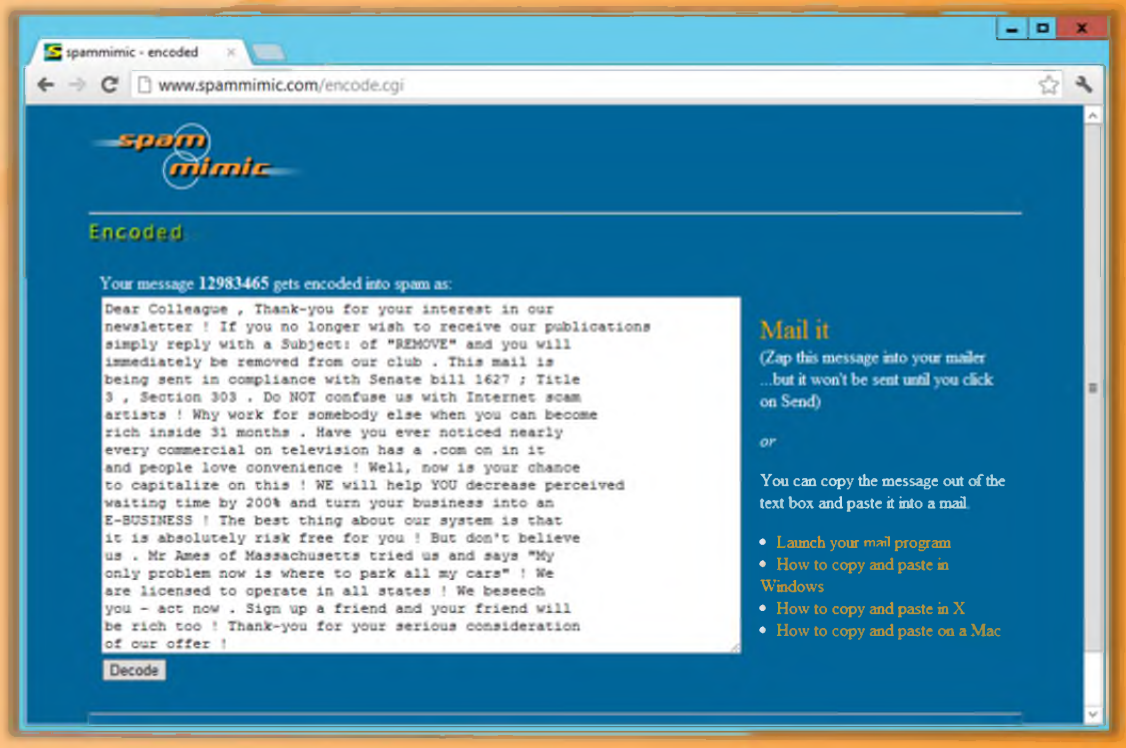
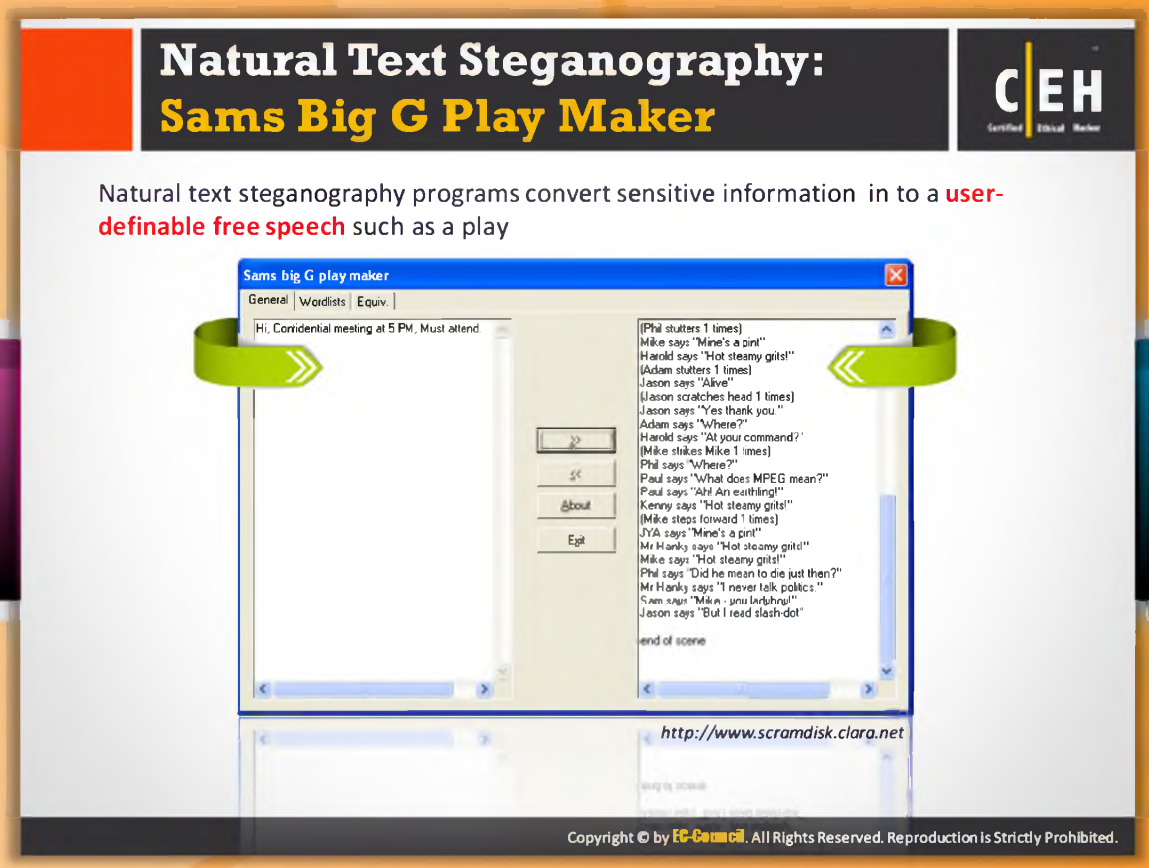


FIGURE 5.78: Spam Mimic Main Page



Natural Text Steganography: Sams Big G Play Maker

Natural text steganography programs convert sensitive information into a user-definable free speech item such as a play. Sams Big G Play Maker helps in performing natural text steganography.

Source: http://www.scramdisk.clara.net

Sams Big G Play Maker is a Windows-based program that is designed for hiding secret messages in the form of an amusing play or conversation. This is usually applicable for small messages. Looking at the **secret message's** output play that is generated using this tool, no one can realize that the output play contains a hidden message.

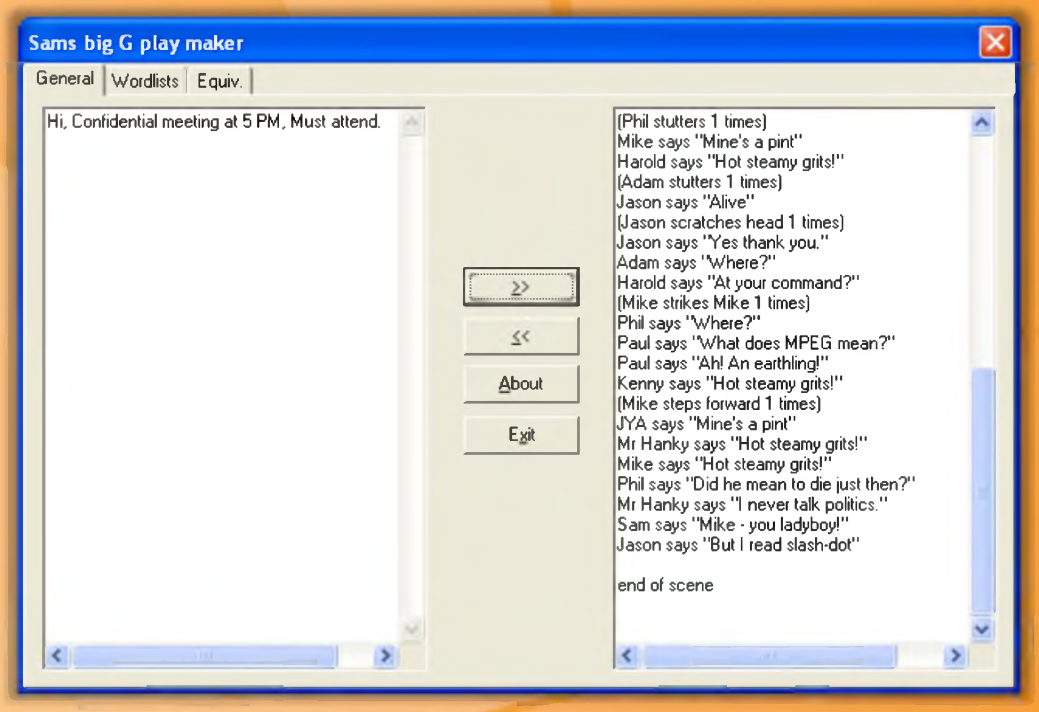
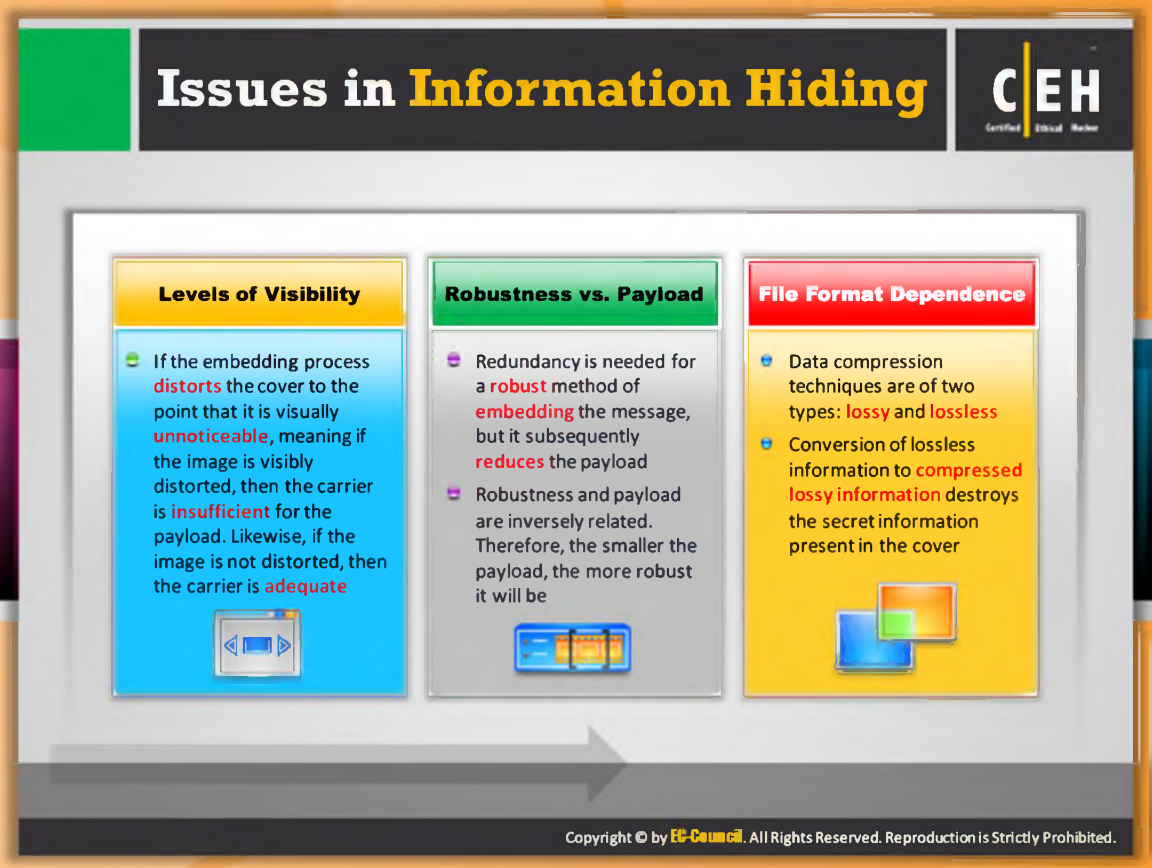


FIGURE 5.79: Sams Big G Play Maker Screenshot



Issues in Information Hiding

The following three sections discuss issues that must be considered when hiding information.

Steganographic File System

In a steganographic file system, a relatively large amount of sensitive information is hidden within an existing host file system. A **steganographic** file system allocates dynamically fragments of hidden information to the unused location on a storage device, thereby allowing the hidden data to be **embedded** within a host file system. It also allows users to give names and password (access keys) for the files. In this method, the data is obfuscated using cryptographic algorithms, but the presence of data is denied without the **corresponding access** key, i.e., given by the user. Without the appropriate access key (password) the attacker cannot get the data of the file.

The following method is used to construct a steganographic file system:

- File system begins with random data.
- The encrypted blocks are written to the pseudorandom locations using the key acquired from the filename and directory password to hide the file blocks in random data. When

the file system continues to be written to, collisions occur and the blocks are overwritten, allowing only a small portion of the disk space to be safely utilized.

- Multiple copies of each block should be written.
- A method to identify the blocks when they are overwritten is also required.

Need for steganographic file systems

Steganographic file systems provide additional protection to the hidden data in a convenient way. With the help of these, users can store their **confidential** (such as trade secrets) or financial information on their systems without any fear. To access the information, the person should hold expressly granted **permissions** and **knowledge** without which he or she cannot access the information in the file. The information hiding techniques not only encrypt the data content but also the presence of data. The data that is within the steganographic file system can only be accessed by the user having the **access key** (granted permissions).

Levels of Visibility

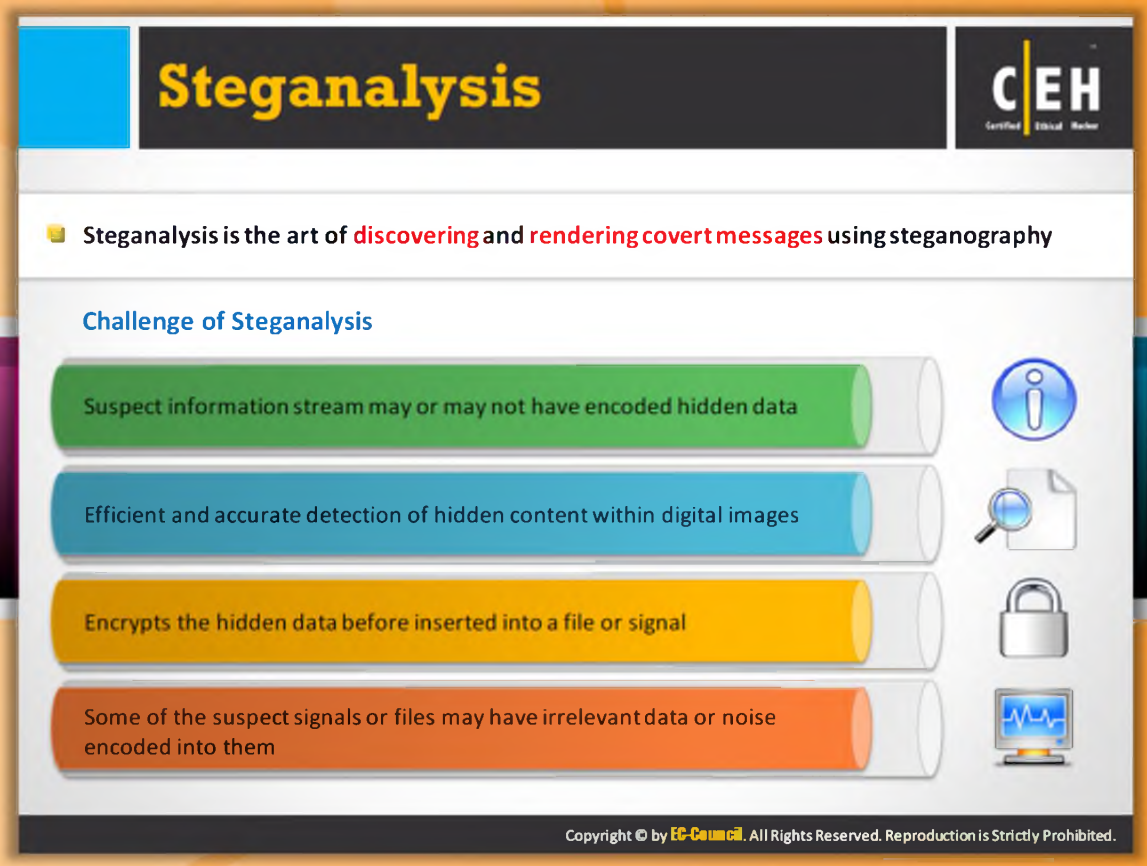
If the embedding process distorts the cover to the point that it is visually unnoticeable, meaning if the image is visibly distorted, then the carrier is insufficient for the payload. Likewise, if the image is not distorted, then the carrier is adequate. The way a message is embedded will determine whether the data is perceptible or not. To reduce the theft of data, the presence of a watermark is often publicized. However, publicizing the presence of a watermark also allows various methods to be implemented to attempt to alter or disable the watermark. When the visibility of the data is increased, the potential for manipulation of the data also increases.

Robustness versus Payload

In order to have a **robust method** of embedding a message, redundancy should be maintained to resist changes made to the cover. However, increasing the robustness of the message means that less space is usable for the payload. Robustness must be weighed against the size of the payload.

File Format Dependence

Conversion of files that have lossless information to compressed files with lossy information can destroy the secret information present in the cover. Some processes embed the data depending on the file format of the carrier, while others do not depend on the file format. The JPEG compression algorithm uses **floating-point** calculations to translate the picture into an array of integers. This conversion process can result in rounding errors that may eliminate portions of the image. This process does not result in any noticeable difference in the image. Nevertheless, embedded data could become damaged. Some other popular algorithms, namely Windows Bitmap (BMP) and **Graphic Interchange Format** (GIF), are considered lossless compressions. The compressed image is an exact representation of the original.



Steganalysis

Steganalysis is the reverse process of **steganography**. It hides the data, while steganalysis is used to detect the hidden data. It determines the encoded hidden message, and if possible, it recovers that message. The message can be detected by looking at variances between bit patterns and unusually large file sizes.

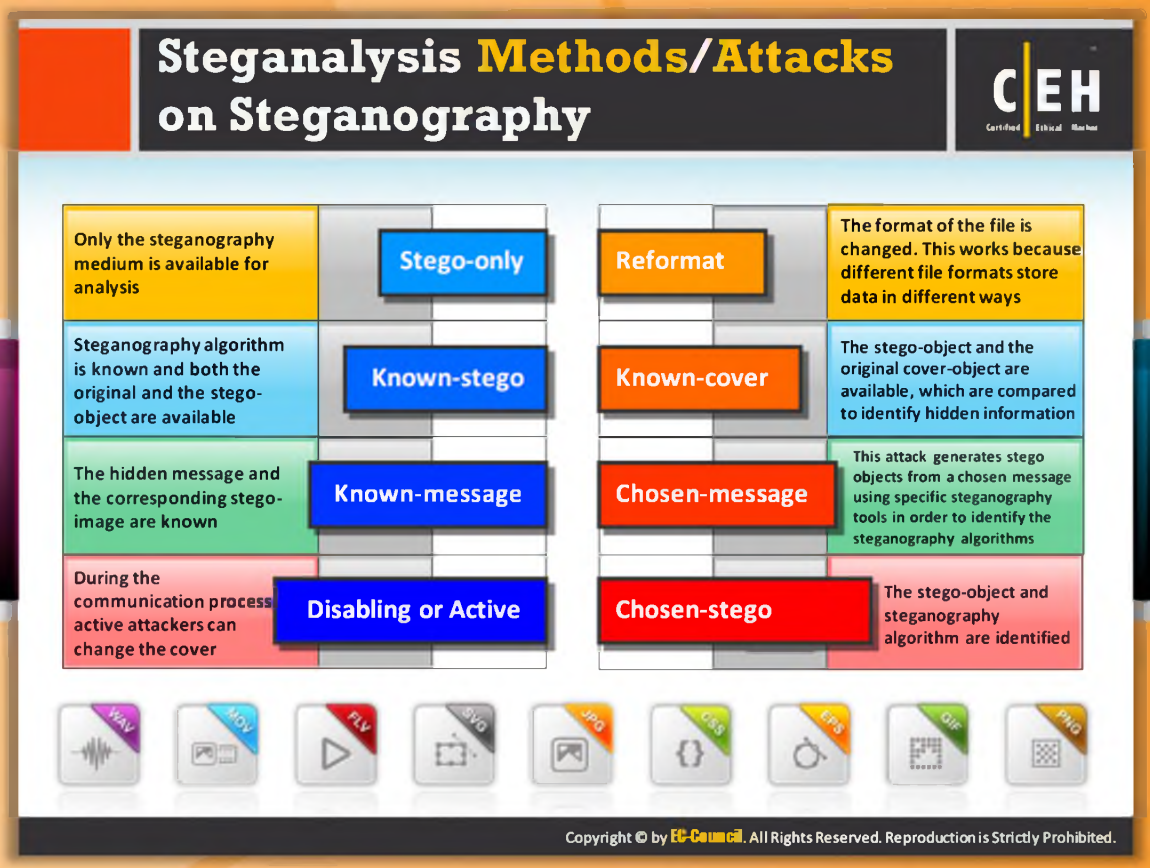
The first step in steganalysis is to discover an image that is suspected of harboring a message. This is considered to be an attack on the hidden information. There are two other types of attacks against steganography: message attacks and **chosen-message attacks**. In the former, the steganalyst has 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.

Cover images disclose more visual clues as compared to stego-images. It is necessary to analyze the stego-images to identify the information that is concealed. 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, a stego-image can be **destroyed** or the **hidden message** can be modified. Some of the data that is hidden behind the images using the Image Domain Tool can prove to be useless.

Challenges of Steganalysis:

- Suspect information stream may or may not have encoded hidden data
- Efficient and accurate detection of hidden content within digital images
- Encrypts the hidden data before inserted into a file or signal
- Some of the suspect signals or files may have **irrelevant data** or noise encoded into them



Steganalysis Methods/Attacks on Steganography

Steganography attacks are split into eight types: stego-only attacks, reformat attacks, known-cover attacks, known-message attacks, known-stego attacks, chosen-stego attacks, chosen-message attacks, and disabling attacks.

Stego-only attack

The stego-only attack takes place when there is only the stego-medium, which carries out the attack. The only way that this attack can be avoided is by detecting and extracting the embedded message.

Reformat attack

In this method the format of the file is changed. This works because different file formats store data in different ways.

Known-cover attack

The known-cover attack is used with the presence of a stego-medium as well as a cover-medium. This would enable a comparison to be made between both the mediums so that the change in the format of the medium can be detected.

Known-message attack

The known-message attack presumes that the message and the stego-medium are present, and the technique by which the message was embedded can be found.

Known-Stego attack

In this attack, the steganography algorithm is known and both the original and stego-object are available.

Chosen-stego attack

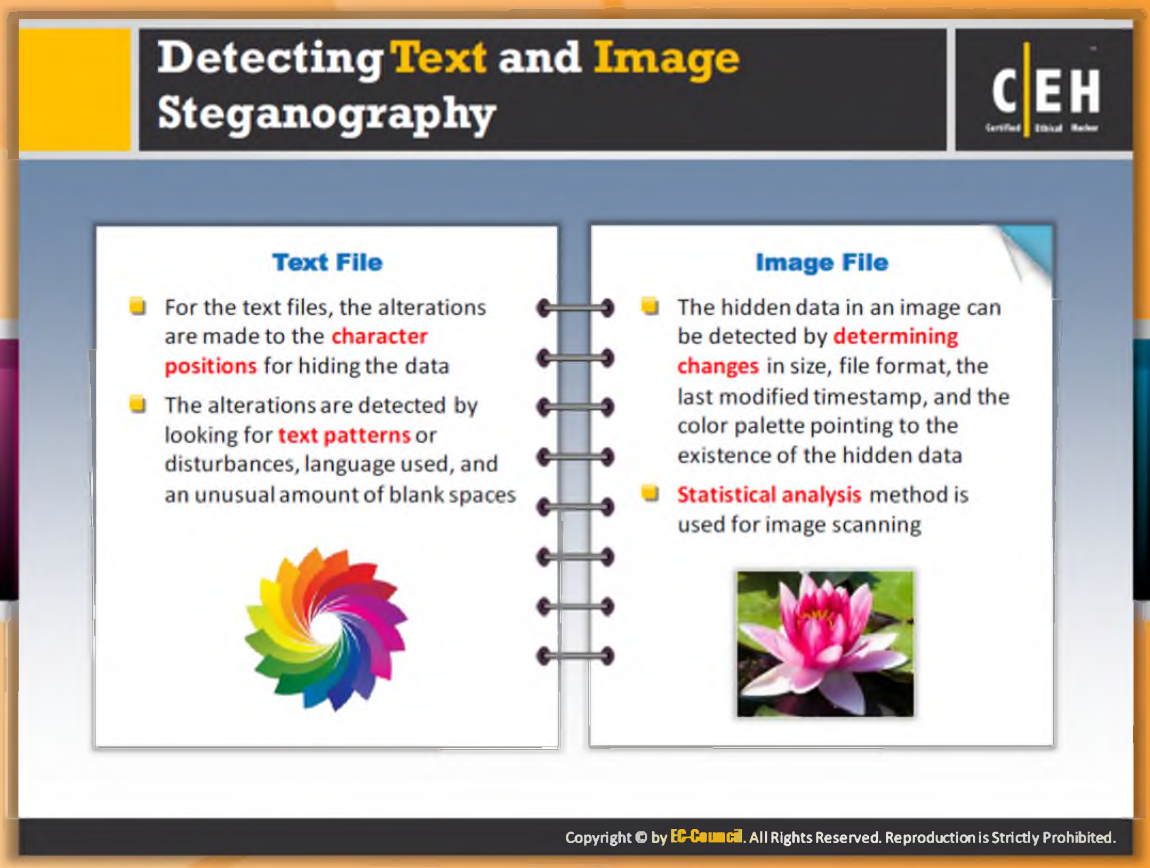
The chosen-stego attack takes place when the forensic investigator generates a stego-medium from the message by using a special tool. Searching for signatures that will enable the detection of other steganography mediums can carry out such an attack.

Chosen-message attack

The steganalyst generates a stego-object from some steganography tool or algorithm of a chosen message. 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.

Disabling or active attacks

These are categorized into six parts, which include blur, noise reduction, sharpen, rotate, resample, and soften. Disabling attacks can smooth transitions and decrease the contrast by averaging the pixels next to the hard edges of the defined lines and the areas where there are significant color transitions. This is otherwise called blurring the stego-medium. Random noise in the stego-medium inserts random-colored pixels to the image. The uniform noise inserts pixels and colors that closely resemble the original pixels. Noise reduction decreases the noise in the image by adjusting the colors and averaging the pixel values. Sharpening is the opposite of the blur effect. It increases contrast between adjacent pixels where there are significant color contrasts that are usually at the edge of objects. Rotation moves the stego medium to give its center a point. Resampling involves what is known as the interpolation process that is used to reduce the raggedness associated with the stego-medium. Resampling is normally used to resize the image. Softening of the stego-medium applies a uniform blur to an image to smooth edges and reduce contrasts and cause less distortion than blurring.



Detecting Text and Image Steganography

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. are used for **hiding sensitive information** from **unauthorized users**. Hidden data is detected in different ways depending on the file used. The following file types require specific methods to detect hidden messages. When a message is hidden in a file in such a way that only the **authorized** user aware of the hidden message can read or recover the message, probably the alteration is applied to the cover or carrier file. The **alteration varies** based on the type of file used as carrier.

Text Files

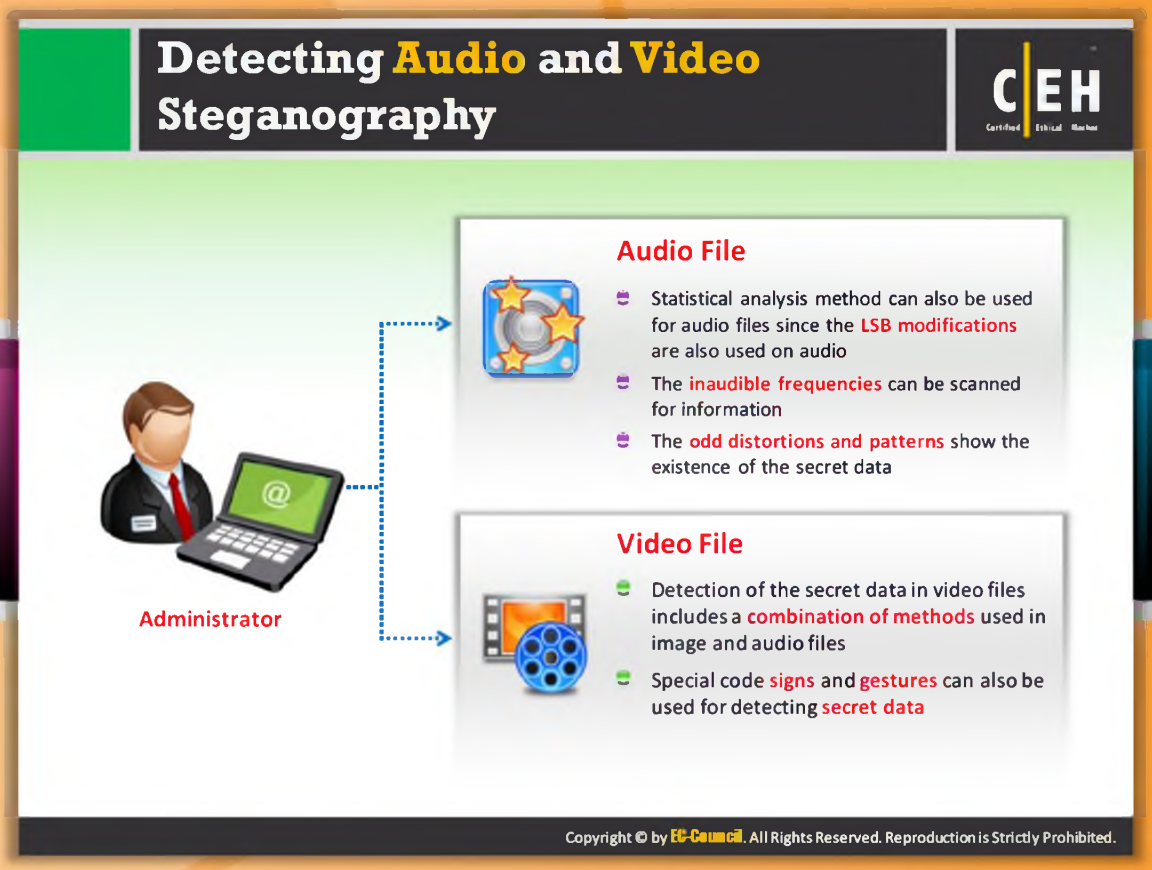
For text files, the alterations are made to the character position for hiding the data. These alterations can be **detected** by looking for text patterns or **disturbances**, the language used, line height, and unusual number of blank spaces.

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.

Statistical analysis methods can be used when scanning an image. Assuming that the least significant bit is more or less random is an incorrect assumption since applying a filter that shows the LSBs can produce a **recognizable** image. Therefore, it can be concluded that LSBs are not random. Rather, they consist of information about the entire image.

Whenever a secret message is inserted 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, the difference between random values and real values can be identified.



Detecting Audio and Video Steganography

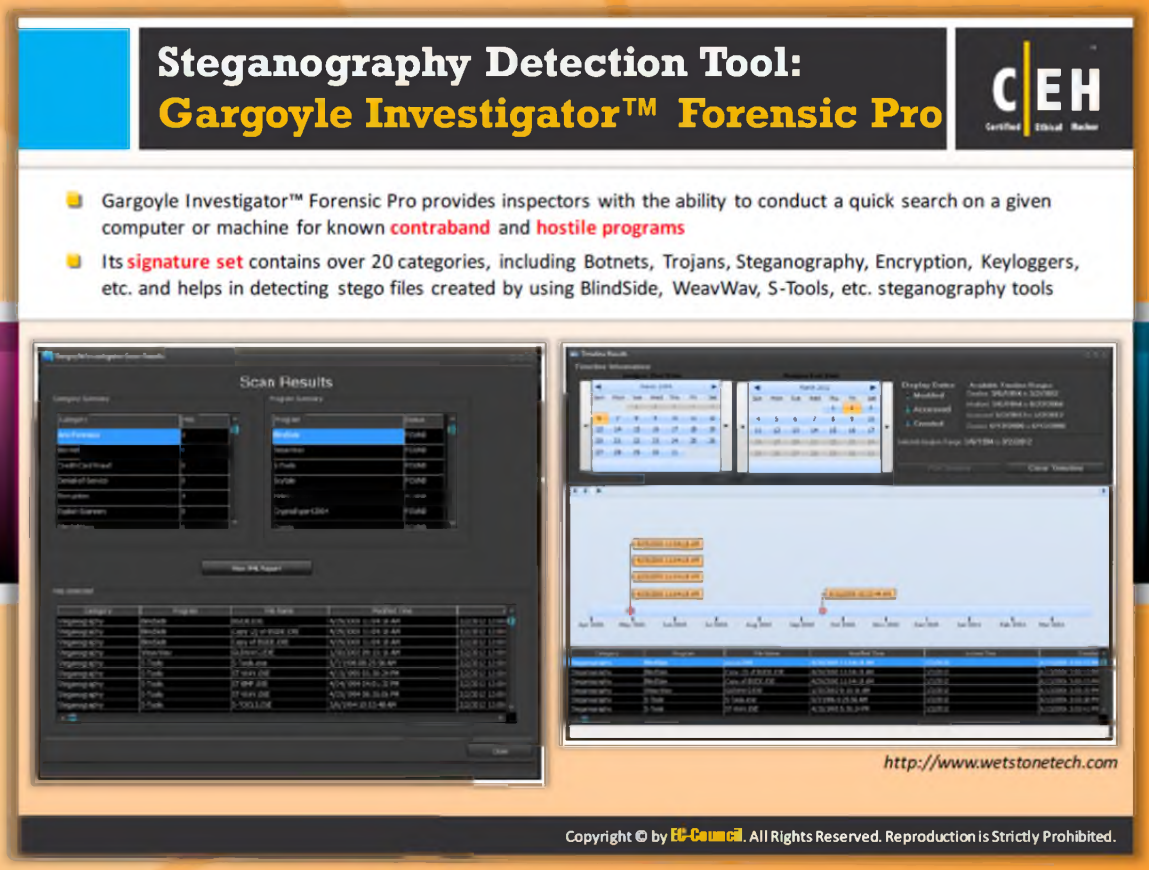
Audio File

In audio steganography, **confidential information** such as private documents and files are embedded in digital sound. The documents that are hidden can be detected by the following ways:

- Statistical analysis method can also be used for audio files since the LSB modifications are also used on audio
- The inaudible frequencies can be scanned for information
- The odd distortions and patterns show the existence of the secret data

Video File

In video **steganography**, confidential information or any kind of files with any extension are hidden in a carrier video file either by using audio steganography or image **steganography tools**. Therefore, the detection of the **secret data** in video files includes a combination of methods used in image and audio files. **Special code** signs and gestures can also be used for detecting secret **data**.



Steganography Detection Tool: Gargoyle Investigator™ Forensic Pro

Source: http://www.wetstonetech.com

Gargoyle Investigator™ Forensic Pro is a tool that conducts quick searches on a given computer or machines for known **contraband** and malicious programs. It is possible to find remnants even though the program has been removed because the search is conducted for the individual files associated with a particular program. Its **signature set** contains over 20 categories, including botnets, Trojans, steganography, encryption, keyloggers, etc. and helps in **detecting stego** files created by using BlindSide, WeavWav, S-Tools, etc. 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, etc.

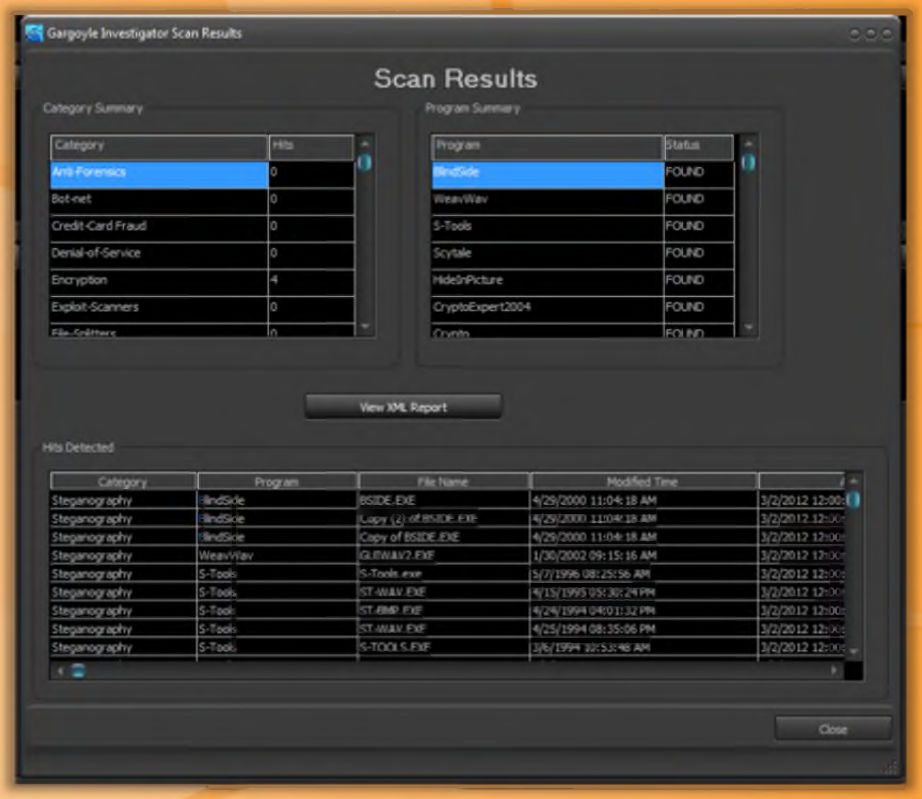


FIGURE 5.80: Gargoyle Investigator™ Forensic Pro Screenshot

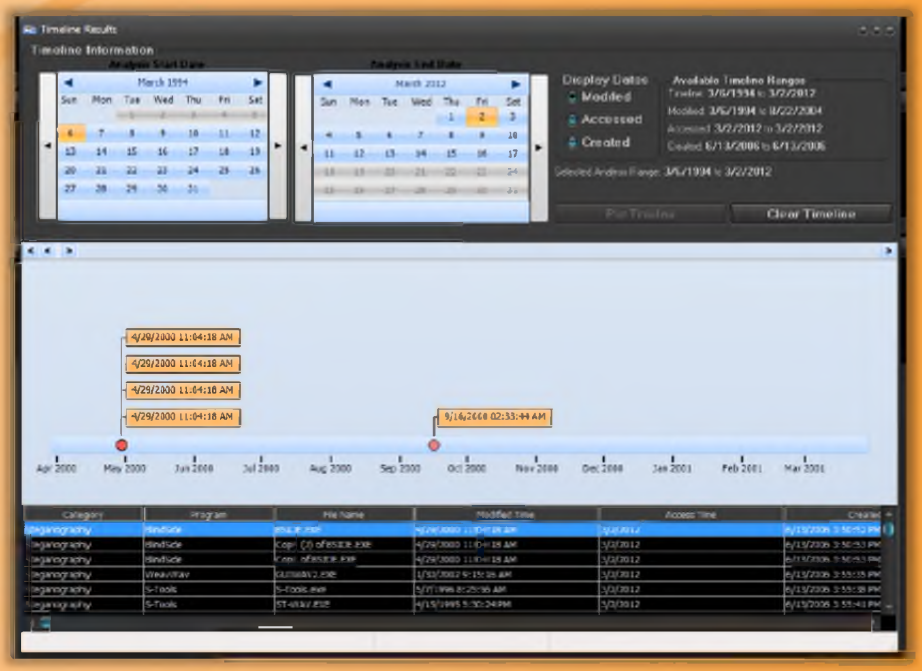
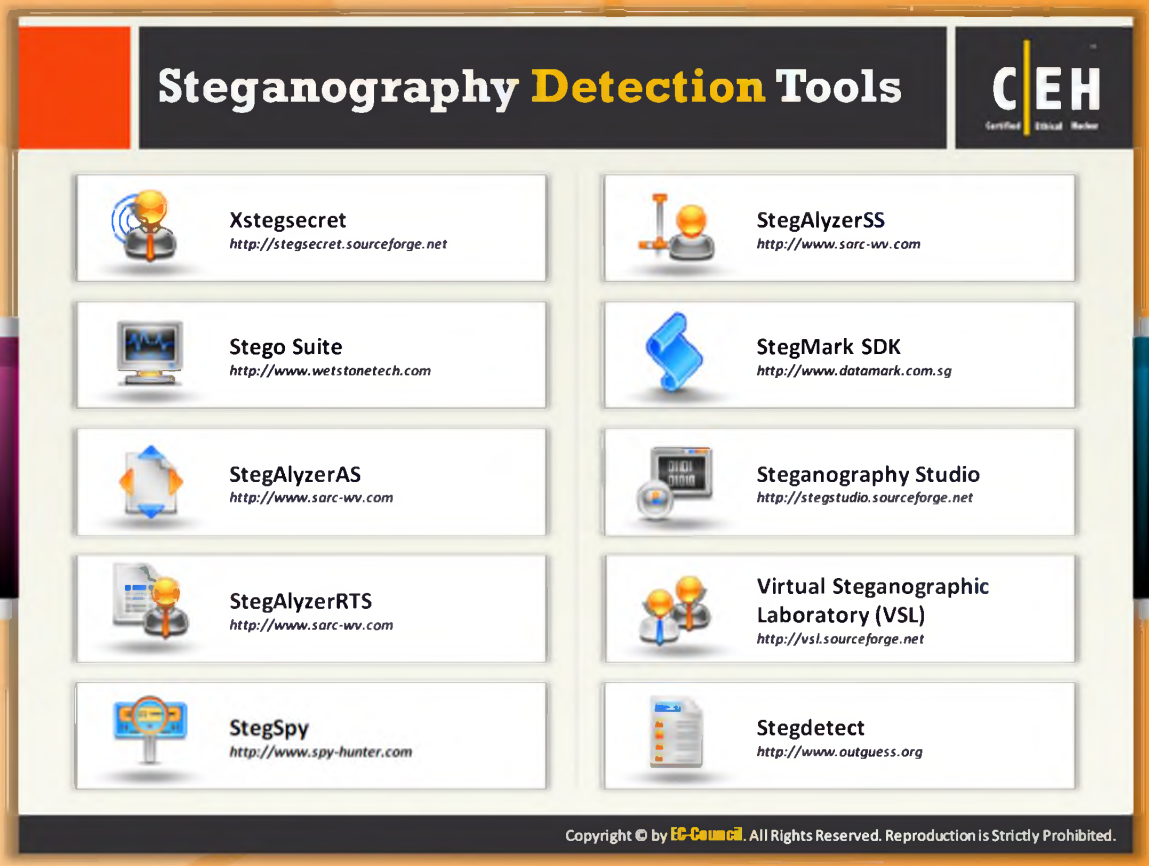


FIGURE 5.80: Gargoyle Investigator™ Forensic Pro Timeline Result Screenshot



Steganography Detection Tools

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 steganography detection **tools**:

- Xstegsecret available at http://stegsecret.sourceforge.net
- Stego Suite available at http://www.wetstonetech.com
- StegAlyzerAS available at http://www.sarc-wv.com
- StegAlyzerRTS available at http://www.sarc-wv.com
- StegSpy available at http://www.spy-hunter.com
- StegAlyzerSS available at http://www.sarc-wv.com
- StegMark SDK available at http://www.datamark.com.sg
- Steganography Studio available at http://sourceforge.net
- Steganographic Laboratory (VSL) available at http://vsl.sourceforge.net
- Stegdetect available at http://www.outguess.org

CEH System Hacking Steps

Once the attacker breaks into the **target network** or computer successfully, he or she tries to hide himself or herself from being detected or **traced out**. Thus, the attacker tries to cover all the tracks or logs that are generated during his or her attempts to gain access to the target network or **computer**.

Cracking Passwords	Hiding Files
Escalating Privileges	Covering Tracks
Executing Applications	Penetration Testing

Why Cover Tracks?

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 or her tracks. The attacker must clear the evidence of "having been there and done the damage." Erasing the intrusion logs, **tracking files**, and attack processes is very crucial for an attacker as the messages can alert the actual owner of the system to change the **security settings** to avoid attacks in the future. If this happens, then the attacker will be left with no chances for relogging into the system for launching the attack. Hence, an attacker needs to destroy the evidence of **intrusion** to maintain the access and evasion. If the attacker covers or deletes their tracks, then he or she can re-login to the system and install **backdoors**. Thus, the attacker can gain users' **sensitive information** such as user names and passwords of bank accounts, email IDs, etc.

The attacker may not wish to delete an entire log to cover his or her tracks as it may require **admin previleges**. If the attacker is able to delete only the **attack event logs**, even then the attacker hides himself or herself from being **detected**.

- 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)

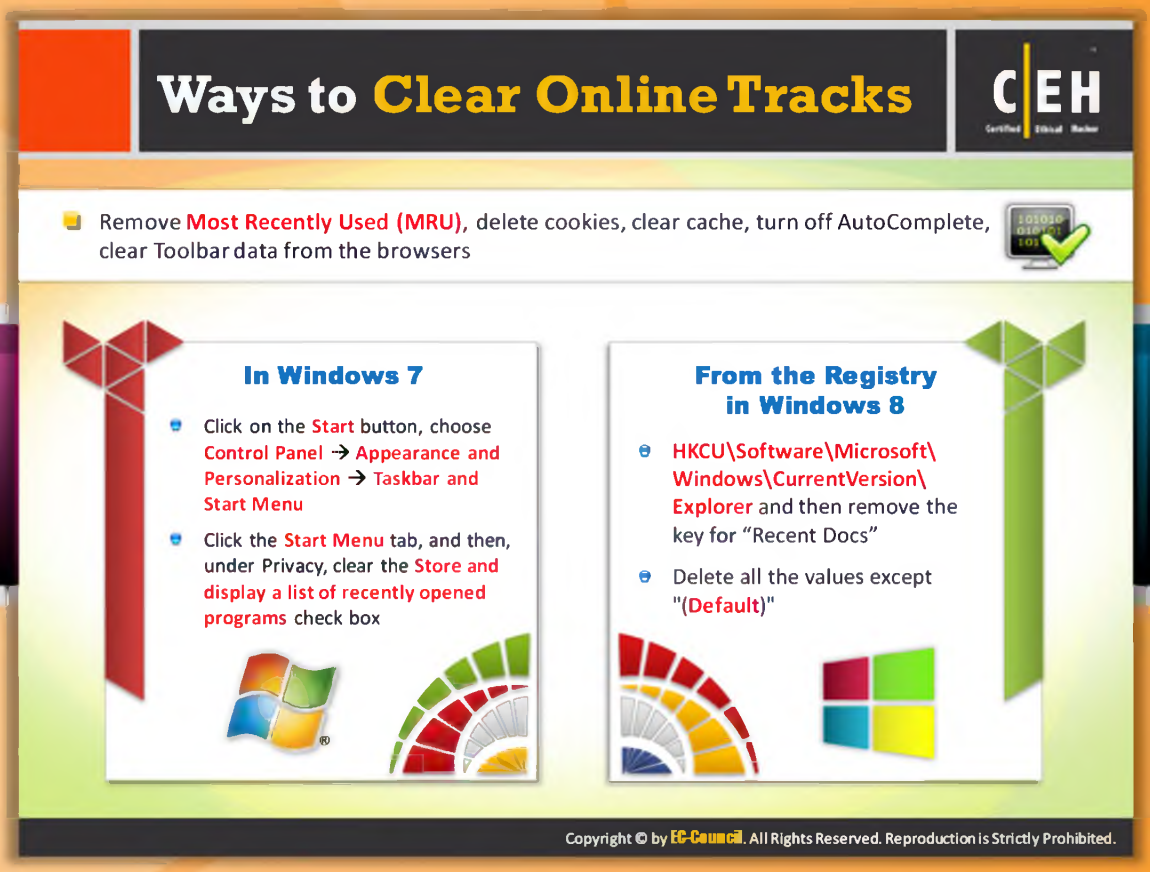
Covering Tracks

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 logins and possible error messages that may have been generated from the attack process. Next, attention is turned to effect any changes so that future logins are not allowed. By manipulating and tweaking the event logs, the **system administrator** can be convinced that the output of his or her system is correct, and that no intrusion or compromise has actually taken place.

Since the first thing a system administrator does to monitor unusual activity is to check the system log files, it is common for intruders to use a utility to modify the system logs. In some cases, **rootkits** can disable and discard all **existing logs**. This happens if the **intruders** intend to use the system for a longer period of time as a launch base for future intrusions, if they remove only those portions of logs that can reveal their presence with the attack.

It is **imperative** for **attackers** to make the system look like it did before they gained access and established backdoors for their use. Any files that have been modified need to be changed back to their original attributes. There are tools for covering one's tracks with regard to the **NT operating system**. Information listed, such as file size and date, is just attribute information contained within the file.

Protecting against an attacker who is trying to cover his or her tracks by changing file information can become difficult. However, it is possible to detect if an attacker has changed file information by calculating a **cryptographic hash** on the file. This type of hash is a **calculation** that is made against the entire file and then **encrypted**.



Ways to Clear Online Tracks

The Internet is the **ultimate resource** to search or to **gather information** related to any topic. Unfortunately, Internet resources are misused by attackers to track others' online activities, which allow them to **launch** an **attack** or **theft**.

There are several ways to clear online tracks:

- Private browsing
- 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

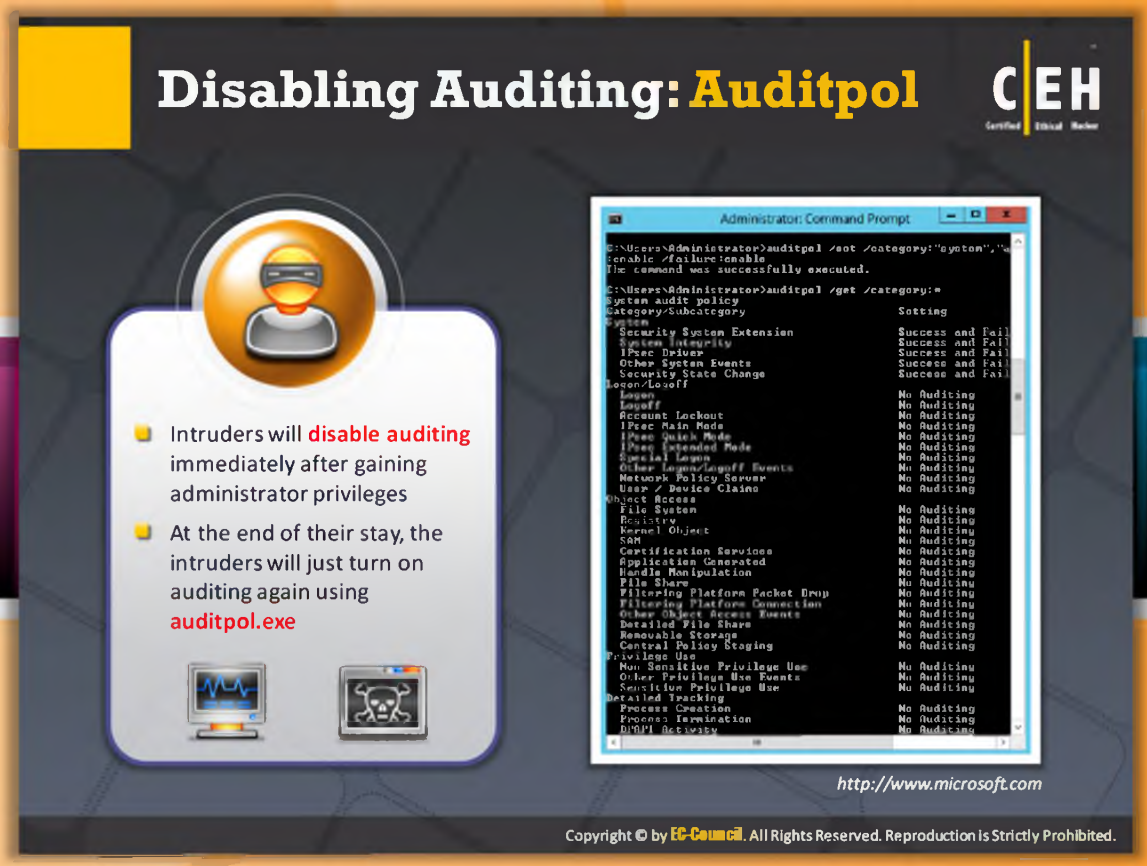
- Delete user JavaScript
- Set up multiple users
- Remove Most Recently Used (MRU)
- Clear Toolbar data from the browsers
- Turn off AutoComplete

In Windows 7

- Click the **Start** button, choose **Control Panel → Appearance and Personalization → Taskbar and Start Menu**.
- Click the **Start Menu** tab, and then, under **Privacy**, clear the **Store and display a list of recently opened programs** check box.

From the Registry in Windows 8

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer and then remove the key for “Recent Docs”
- Delete all the values except "(Default)"



Disabling Auditing: Auditpol

Source: http://www.microsoft.com

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

Windows **auditing 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 or she is trying to compromise before proceeding with his or her plans.

Tool **Auditpol.exe** is a part of the **NT resource kit** and can be used as a simple command-line utility to find out the audit status of the target system and also make changes to it.

The attacker would need to install the utility in the **WINNT directory**. He or she can then establish a null session to the target machine and run the command:

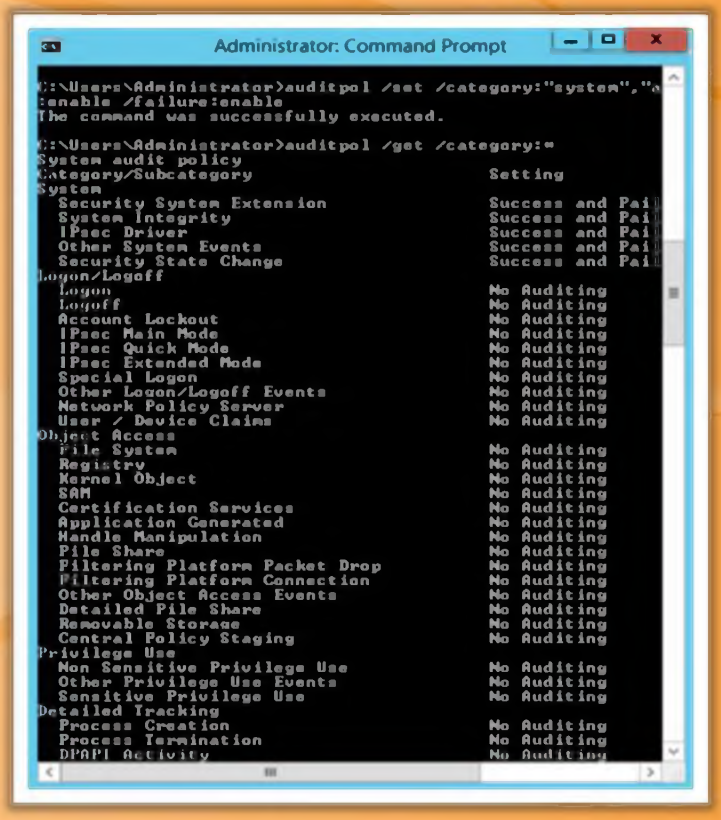
```
C:\> auditpol \\<ip address of target>
```

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 his or her actions. He or she can choose to hide the **registry keys** changed later on.

The moment the intruders gain **administrative privileges**, they disable auditing with the help of auditpol.exe. Once their work is done, after logout intruders again turn on the auditing by using same tool: audit.exe.



Covering Tracks Tool: CCleaner

Source: http://www.piriform.com

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

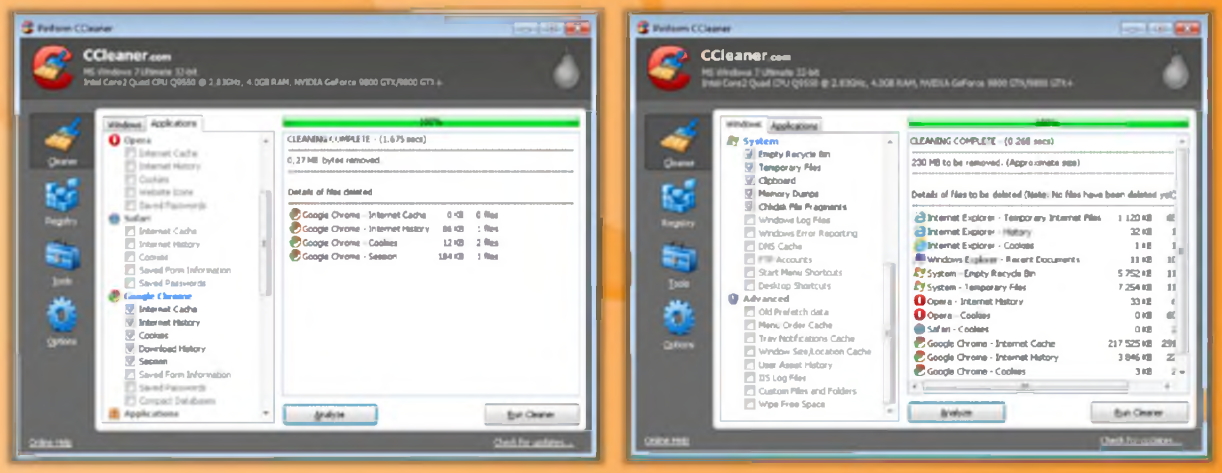


FIGURE 5.82: CCleaner Screenshot

Covering Tracks Tool: MRU-Blaster

Source: http://www.brightfort.com

MRU-Blaster is a program that allows you to clean most recently used lists on the system, temporary Internet files, and **cookies**. **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**. **MRU-Blaster** safely handles cleaning up of "**usage tracks**" and other remnants that most programs leave behind.

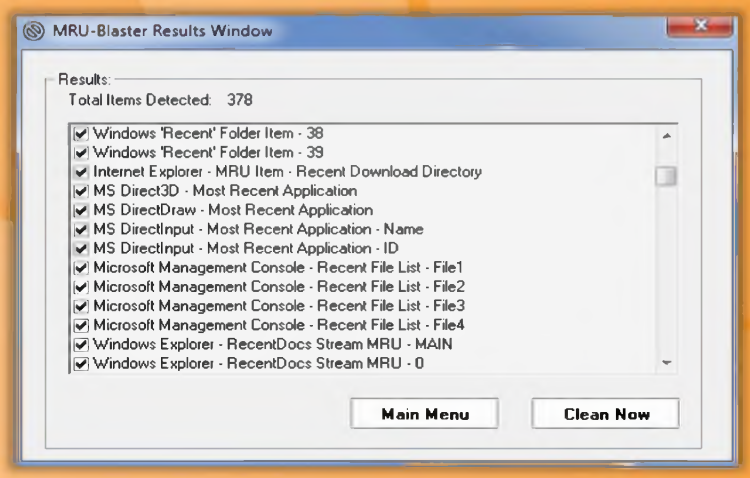


FIGURE 5.83: MRU-Blaster Results Window

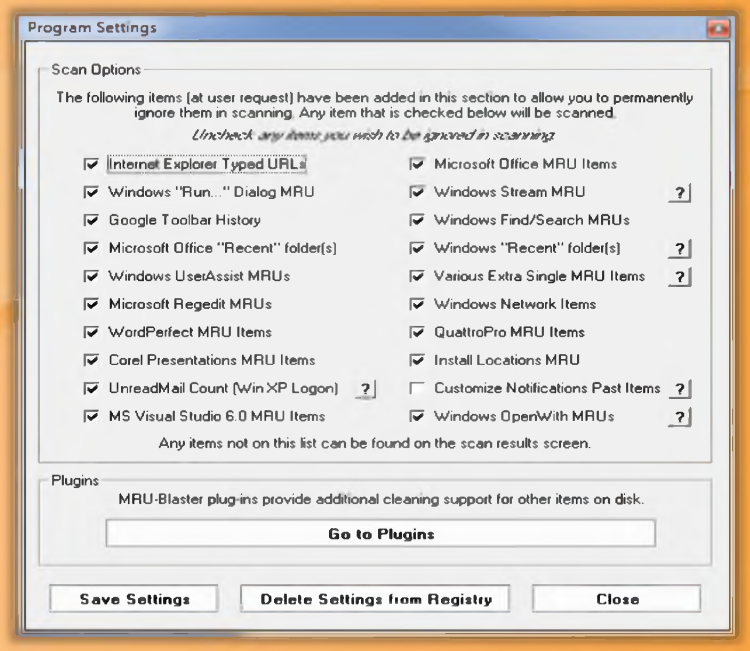
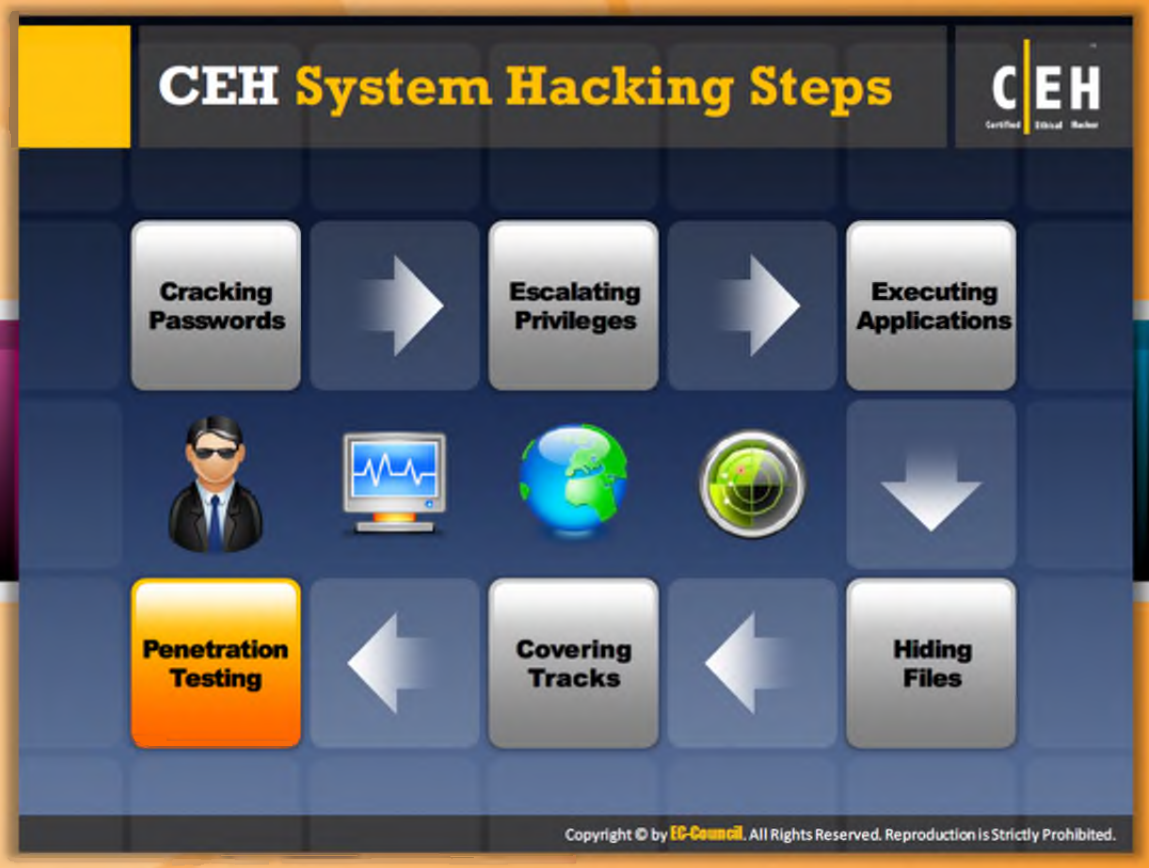


FIGURE 5.84: MRU-Blaster Program Settings

Track Covering Tools

Track covering tools protects your personal information throughout your **Internet browsing** by cleaning up all the tracks of **Internet activities** on the computer. They free cache space, delete cookies, clear Internet history shared temporary files, delete logs, and discard junk. A few of these **tools** are listed as follows

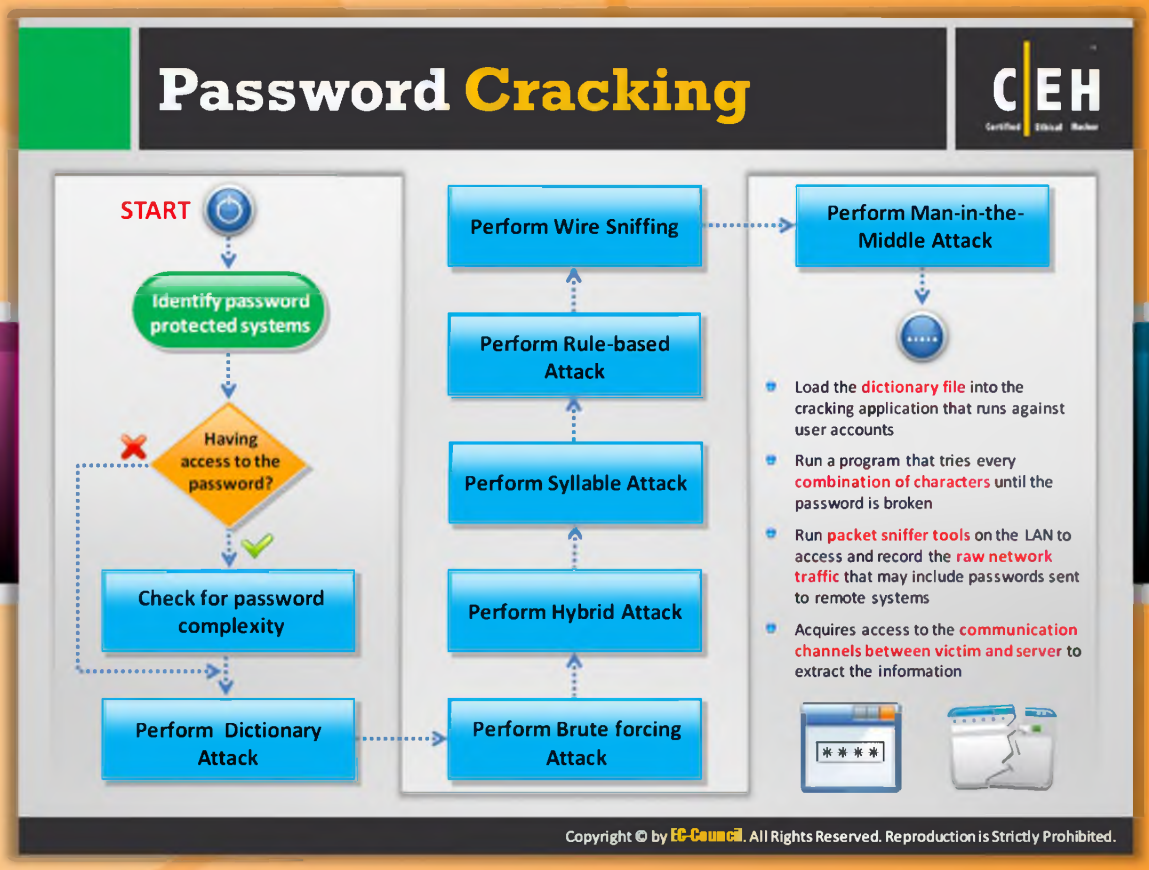
- Wipe available at http://privacyroot.com
- Tracks Eraser Pro available at http://www.acesoft.net
- BleachBit available at http://bleachbit.sourceforge.net
- AbsoluteShield Internet Eraser Pro available at http://www.internet-track-eraser.com
- Clear My History available at http://www.hide-my-ip.com
- EvidenceEraser available at http://www.evidenceeraser.com
- WinTools.net Professional available at http://www.wintools.net
- RealTime Cookie & Cache Cleaner (RtC3) available at http://www.kleinsoft.co.za
- AdvaHist Eraser available at http://www.advacrypt.cjb.net
- Free Internet Window Washer available at http://www.eusing.com



CEH System Hacking Steps

As a pen tester, you should evaluate the **security posture** of the target network or system. To evaluate the security, you should try to **break the security** of your system by simulating various attacks on the system, just like an attacker would. There are certain steps that you need to follow to conduct a system **penetration test**. This section will teach you how to conduct a system **hacking penetration test**.

Cracking Passwords	Hiding Files
Escalating Privileges	Covering Tracks
Executing Applications	Penetration Testing



Password Cracking

In an attempt to **hack a system**, the attacker initially tries to crack the password of the system, if any. Therefore, as a pen tester, you should also try to crack the password of the system. To crack the **password**, follow these steps:

Step1: Identify password protected systems

Identify the target system whose **security needs** to be evaluated. Once you identify the system, check whether you have access to the password, that means a stored password. If the password is not stored, then try to perform various **password cracking attacks** one after the other on the target system.

Step 2: Perform a dictionary attack

Perform a dictionary attack by loading the **dictionary file** into the **cracking application** that runs against user accounts. Run the cracking application and observe the results. If the application is allowing you to log in to the system, it means that the **dictionary file** contains the respective password. If you are not able to log in to the system, then try other **password-cracking** techniques.

Step3: Perform wire sniffing

Run **packet sniffer tools** on the LAN to access and record the **raw network traffic** that may include passwords sent to remote systems.

Step4: Perform a rule-based attack

Try to obtain the password by performing a **rule-based** attack.

Step5: Perform a syllable attack

Try to extract the password by performing a syllable attack. This attack is a combination of a brute force attack and a dictionary attack.

Step6: Perform a hybrid attack

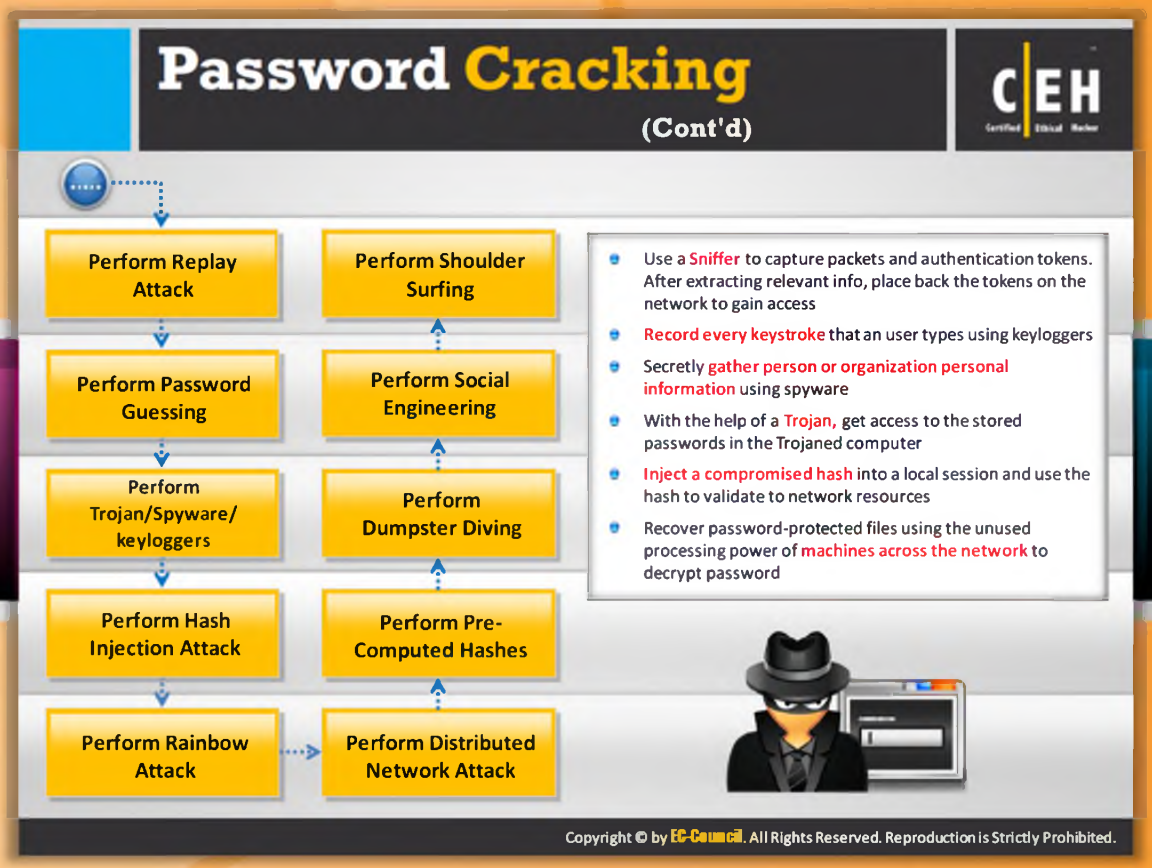
Try to perform a **hybrid attack**. This attack is used to find passwords that are a dictionary word with combinations of characters prepended or post pended to them.

Step7: Perform a brute force attack

You should try every **possible combination** of characters until a password is found.

Step8: Perform a man-in-the-middle attack

Try to **acquire access** to the communication channels between victim and server to extract the information.



Password Cracking (Cont'd)

Step 9: Perform a replay attack

Try to intercept the data in the communication and **retransmit** it.

Step 10: Perform password guessing

Try to guess the possible **combinations** of **passwords** and apply them.

Step11: Perform TrojansSpyware/keyloggers

Use malicious applications or malware such as Trojan/spyware/keyloggers to steal passwords.

Step12: Perform Hash Injection Attack

Inject a **compromised hash** into a local session and use the hash to validate to network resources.

Step 13: Perform a rainbow attack

Use a rainbow table that stores pre-computed hashes to **crack the hashed** password.

Step 14: Perform a distributed network attack

Recover password-protected files using the unused **processing power** of machines across the network to decrypt passwords.

Step 15: Perform pre-computed hashes

Use **pre-computed hashes** to crack passwords.

Step 16: Perform dumpster diving

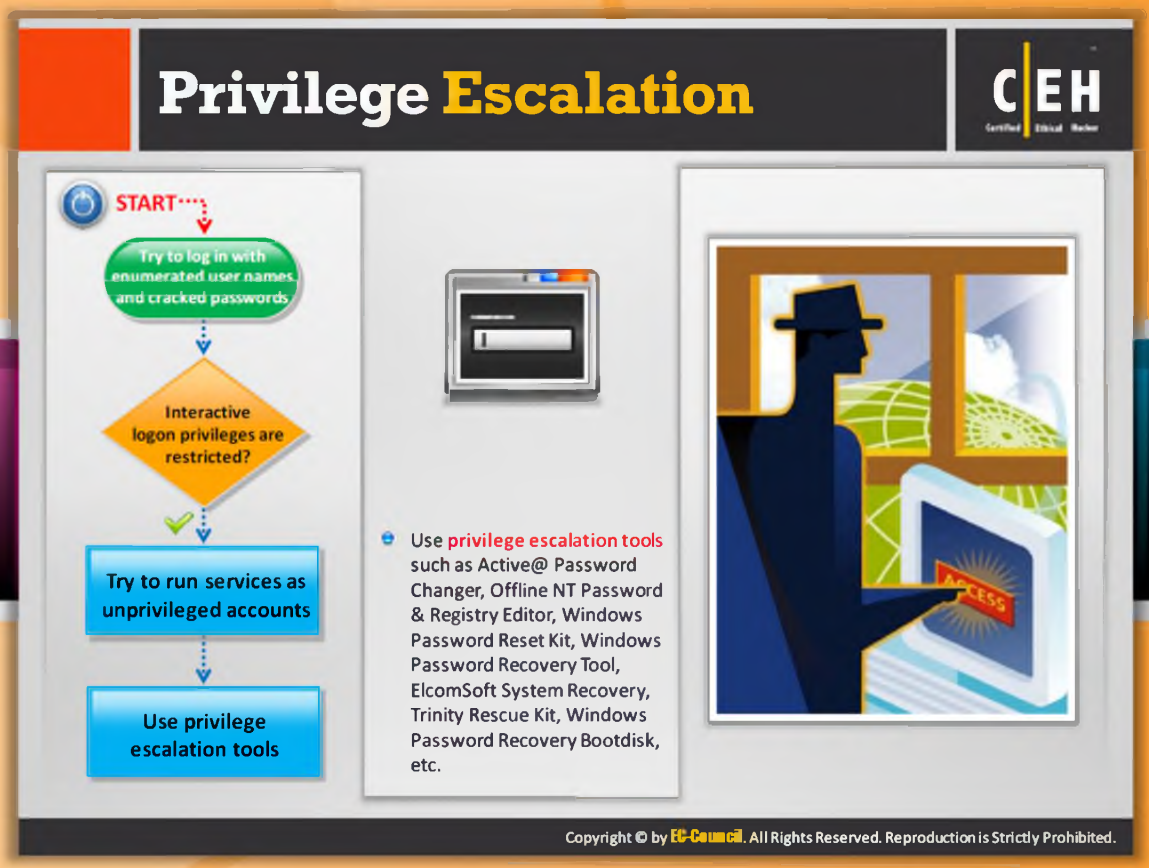
Check the trash bin of your target to check whether you find **confidential passwords** anywhere.

Step 17: Perform social engineering

Use the social engineering technique to **gain passwords**.

Step 18: Perform shoulder surfing

Check whether you can **steal the password** by using **shoulder surfing**.



Privilege Escalation

Once the attacker gains the **system password**, he or she then tries to escalate their **privileges** to the administrator level so that they can install **malicious programs** or malware on the target system and thus **retrieve sensitive information** from the system. As a **pen tester**, you should hack the system as a normal user and then try to escalate your privileges. The following are the steps to perform **privilege escalation**:

Step1: Try to log in with enumerated user names and cracked passwords

Once you crack the password, try to log in with the password obtained in order to gain access to the system. Check whether **interactive logon privileges** are restricted.

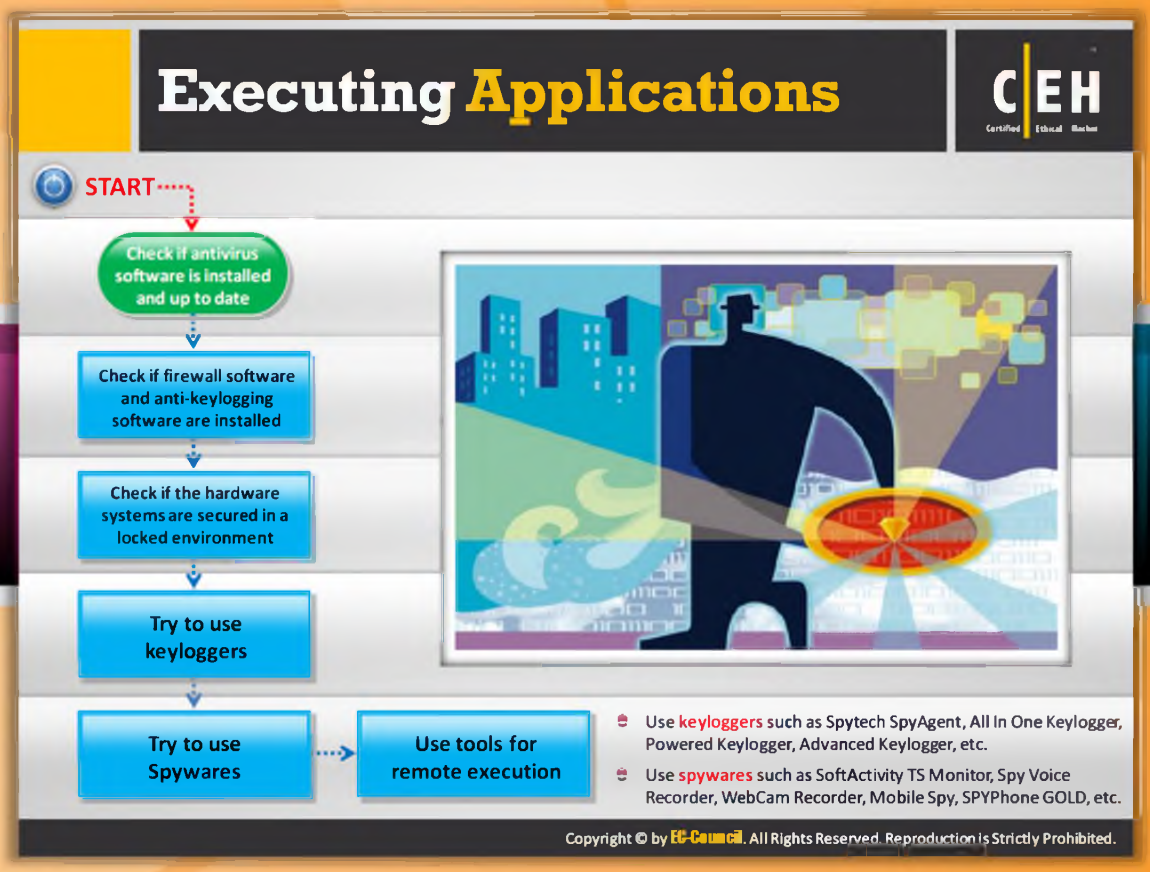
If YES, then try to run the services as **unprivileged accounts**.

Step2: Try to run services as unprivileged accounts

Before trying to **escalate your privileges**, try to run services and check whether you have permissions to run services or not. If you can run the services, then use privilege escalation tools to obtain **high-level privileges**.

Step3: Use privilege-escalation tools

Use privilege-escalation tools such as Active@ Password Changer, Offline NT Password & Registry Editor, Windows Password Reset Kit, Windows Password Recovery Tool, ElcomSoft System Recovery, Trinity Rescue Kit, Windows Password Recovery Bootdisk, etc. These tools will help you to **gain higher level privileges**.



Executing Applications

Pen testers should check the target systems by executing some applications in order to find out the loopholes in the system. Here are the steps to check your system when you choose certain applications to be executed to determine loopholes.

Step1: Check antivirus installation on the target system

Check if antivirus software is installed on the target system and if installed, check that it is up-to-date or not.

Step2: Check firewall anti-keylogging software installation on the target system

Check if firewall software and anti-keylogging software is installed or not.

Step3: Check the hardware system

Check if the hardware systems are secured in a locked environment.

Step4: Use keyloggers

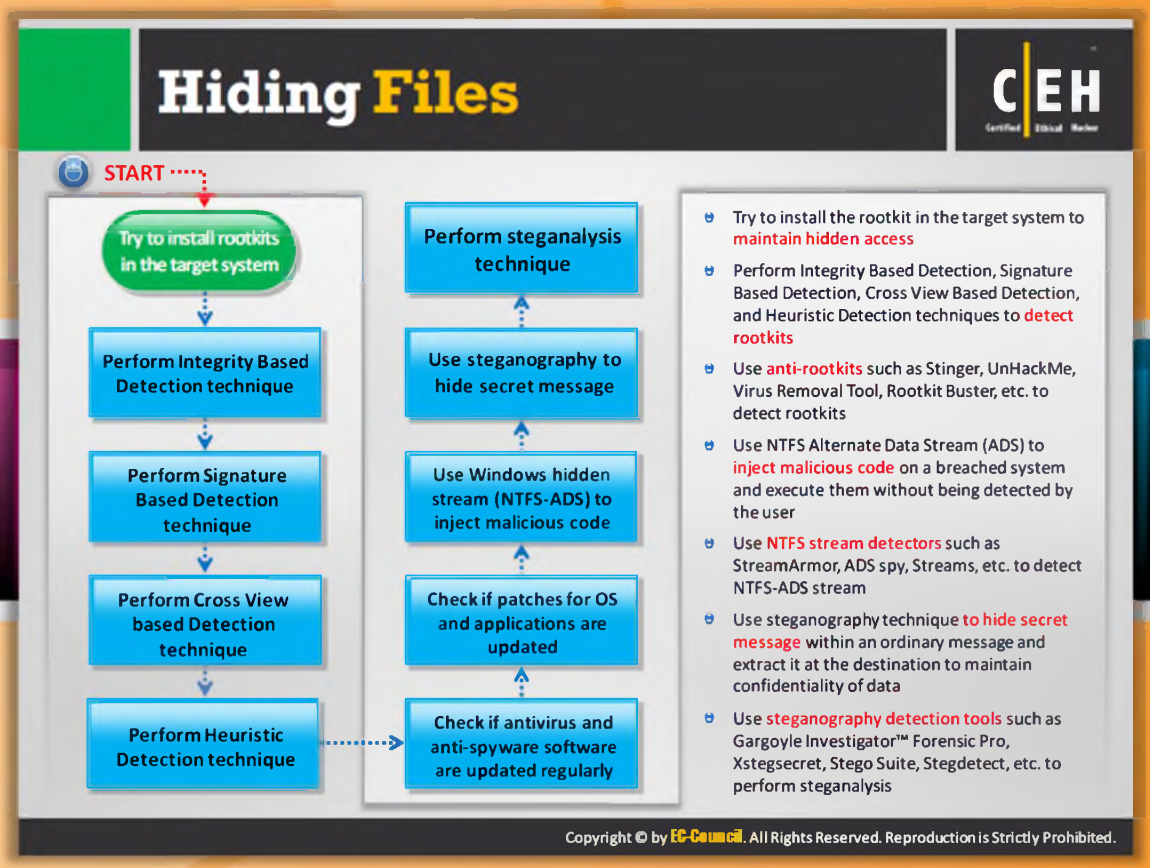
Try to install and use keyloggers on the system in order to record keystrokes. Use keyloggers such as Spytech SpyAgent, All In One Keylogger, Powered Keylogger, Advanced Keylogger, etc.

Step5: Use spyware

Try to install and use **spyware** on the system in order to **monitor** the activities on the system. Use spyware such as SoftActivity TS Monitor, Spy Voice Recorder, WebCam Recorder, Mobile Spy, SPYPhone GOLD, etc.

Step6: Use tools for remote execution

Try to install and use tools for **remote execution**.



Hiding Files

An attacker **installs rootkits** to maintain hidden access to the system. You should follow pen testing steps for **detecting hidden files** on the target system.

Step1: Install rootkits

First try to install the **rootkit** in the target system to maintain hidden access.

Step2: Perform integrity-based Detection techniques

Perform integrity-based detection, signature-based detection, cross-view-based detection, and heuristic detection techniques to detect **rootkits**.

Step3: Use anti-rootkits programs

Use anti-rootkits such as Stinger, UnHackMe, Virus Removal Tool, Rootkit Buster, etc. to detect rootkits.

Step4: Use NTFS Alternate Data Streams (ADSs)

Use NTFS **Alternate Data Streams** (ADSs) to inject malicious code on a breached system and execute it without being detected by the user.

Step5: Use NTFS stream detectors

Use NTFS stream detectors such as StreamArmor, ADS spy, Streams, etc. to detect **NTFS-ADS** streams.

Step6: Use steganography technique

Use steganography techniques to **hide secret messages** within an ordinary message and extract it at the destination to maintain confidentiality of data.

Step7: Use steganography detection

Use **steganography** detection tools such as Gargoyle Investigator™ Forensic Pro, Xstegsecret, Stego Suite, Stegdetect, etc. to perform steganalysis.

Covering Tracks

The **pen tester** should whether he or she can cover the tracks that he or she has made during simulating the attack to conduct **penetration testing**. To check whether you can cover tracks of your activity, follow these steps:

Step1: Remove web activity tracks

First, remove the web **activity tracks** such as such as MRU, cookies, cache, temporary files, and history.

Step2: Disable auditing

Try to disable auditing on your **target system**. You can do this by using tools such as Auditpol.

Step3: Tamper with log files

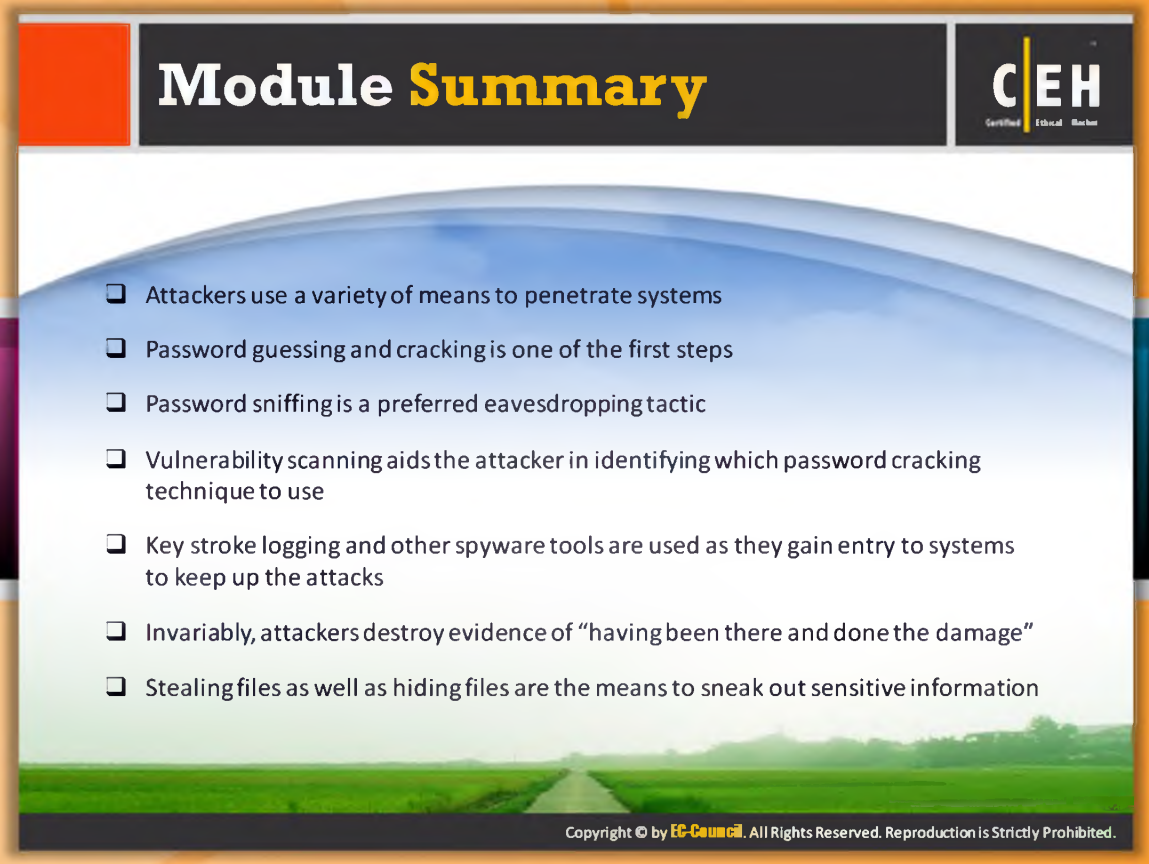
Try to tamper with log files such as **event log files**, server log files, and **proxy log files** with log poisoning or log flooding.

Step4: Use track covering tools

Use **track covering tools** such as CCleaner, MRU-Blaster, Wipe, Tracks Eraser Pro, Clear My History, etc.

Step5: Try to close all remote connections to the victim machine

Step6: Try to close any opened ports



Module Summary

- **Attackers** use a variety of means to **penetrate** systems.
- Password guessing and cracking is one of the first steps.
- Password sniffing is a preferred eavesdropping tactic.
- Vulnerability scanning aids the attacker in identifying which password cracking technique to use.
- Keystroke logging and other **spyware tools** are used to gain entry to systems to keep up attacks.
- Invariably, attackers destroy evidence of "having been there and done the damage."
- Stealing files as well as hiding files are the means to sneak out **sensitive** information.