

15
Marks

15
Marks

OUTLINE

- Introduction
- Password Cracking
- Key loggers and Spywares
- Virus and Worms
- Steganography
- DoS and DDoS Attacks
- SQL Injection
- Buffer Over Flow
- Attacks on Wireless Networks
- Phishing
- Identity Theft (ID Theft)

1. Introduction

Reconnaissance

Scanning

Gaining Access

Maintaining Access

Clearing Track

1.1 Reconnaissance

- The penetration tester collects maximum information about the target machine in order to be able to conduct an effective penetration test.
- The tools used for reconnaissance :
 - Google dork
 - Harvester
 - WHOIS
 - Netcraft
 - Nslookup
 - Dig
 - GHBA
 - MetaGoofil
 - Threatagent drone
 - Social engineering

1.2 Enumeration Tools

- Process of gathering information from the system without logging on.
- Usernames, device information, router information, etc
- Example:
 - [DumpSec](#)

1.3 Bulk Network Scanning

- Port scanning and vulnerability scanning
 1. Port scanning – identify open ports and types of services
 2. Vulnerability scanning – identify weaknesses in software and running services

1.4 Tools used to explore vulnerabilities

1. NMAP
2. Nessus
3. Scanning
4. Enumeration
5. Vulnerability detection
6. Nikto

1.5 Tools used to cover tracks

Steps involved:

1. Disable auditing
2. Clear logs
3. Modify logs, registry files
4. Remove all files or folders created

Simple ways to achieve this :

1. Incognito window
2. InPrivacy
3. Do Not Track
4. Ccleaner
5. PrivaZer Free

2. Password Cracking



2.1 Password Cracking



- Password cracking is the process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms that guess passwords.
- Employs a number of techniques to achieve its goals.
- Involve either comparing stored passwords against word list or use algorithms to generate passwords that match.

2.1.1 The purpose of password cracking

1. To recover a forgotten password.
2. As a preventive measure by system administrator to check for easily crackable passwords. (Testing)
3. To gain unauthorized access to a system.

2.1.2 What is password strength?

- Password strength is the measure of a password's efficiency to resist password cracking attacks.
- The strength of a password is determined by;
 - **Length**: the number of characters the password contains.
 - **Complexity**: does it use a combination of letters, numbers, and symbol?
 - **Unpredictability**: is it something that can be guessed easily by an attacker?

2.1.2 What is password strength?

- We will use three passwords namely

1. *password*

2. *password1*

3. *#password1\$*

**** The higher the strength number, better the password.**

Password: ✓

Password (again): ✓

Strength (why?): **Very Weak (1/100)** Password Generator

password

Password: ✓

Password (again): ✓

Strength (why?): **Weak (28/100)** Password Generator

password1

Password: ✓

Password (again): ✓

Strength (why?): **Strong (60/100)** Password Generator

#password1\$

2.1.2 Making use of md5 encryption

- Online md5 hash generator

<https://www.md5hashgenerator.com/>

Password	MD5 Hash	Cpanel Strength Indicator
password	5f4dcc3b5aa765d61d8327deb882cf99	1
password1	7c6a180b36896a0a8c02787eeafb0e4c	28
#password1\$	29e08fb7103c327d68327f23d8d9256c	60

2.1.2 Making use of MD5

- Crack the hashes : <https://www.md5online.org/md5-decrypt.html>

The value of **5f4dcc3b5aa765d61d8327deb882cf99** resolves to -> **password**

The value of **7c6a180b36896a0a8c02787eeafb0e4c** resolves to -> **password1**

Could not resolve the value of **29e08fb7103c327d68327f23d8d9256c** md5 hash.

2.1.2 Weak password

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "<Company Name>", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

2.1.2 Strong password

- Contain both upper- and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, @#\$%^&*()_+|~-=\{}[]:~<>?.,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.
- Try to create passwords that can be easily remembered.
- One way to do this is create a password based on a song title, affirmation, or other phrase.
- For example, the phrase might be: "This May Be One Way To Remember"
- and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

2.1.2 Random password

- Include Symbols:(e.g. @\$%)
- Include Numbers:(e.g. 123456)
- Include Lowercase Characters:(e.g. abcdefgh)
- Include Uppercase Characters:(e.g. ABCDEFGH)
- Exclude Similar Characters:(e.g. i, l, 1, L, o, 0, O)
- Exclude Ambiguous Characters: ({ } [] () / \ ' " ` ~ , ; : . < >)
- Generate On The Client Side:(do NOT send across the Internet)
- Auto-Select:(select the password automatically)

2.1.2 Password strength checker

Not secure | passwordmeter.com

The Password Meter

Agendum Scale
Data Optimize & Parallelize OPEN

Test Your Password		Minimum Requirements	
Password:	<ul style="list-style-type: none">Minimum 8 characters in lengthContains 3/4 of the following items:<ul style="list-style-type: none">Uppercase LettersLowercase LettersNumbersSymbols	
Hide:	<input checked="" type="checkbox"/>		
Score:	100%		
Complexity:	Very Strong		

Additions	Type	Rate	Count	Bonus
<input checked="" type="checkbox"/> Number of Characters	Flat	$+(n*4)$	12	+ 48
<input checked="" type="checkbox"/> Uppercase Letters	Cond/Incr	$+/((len-n)*2)$	1	+ 22
<input checked="" type="checkbox"/> Lowercase Letters	Cond/Incr	$+/((len-n)*2)$	6	+ 12
<input checked="" type="checkbox"/> Numbers	Cond	$+(n*4)$	4	+ 16
<input checked="" type="checkbox"/> Symbols	Flat	$+(n*6)$	1	+ 6
<input checked="" type="checkbox"/> Middle Numbers or Symbols	Flat	$+(n*2)$	4	+ 8
<input checked="" type="checkbox"/> Requirements	Flat	$+(n*2)$	5	+ 10

kaspersky password checker

EN EN FAQ

.....

✓ Nice password!

- Your password is hack-resistant.
- Your password does not appear in any databases of leaked passwords

Your password will be bruteforced with an average home computer in approximately...

41 years

2.2 Classification of password cracking

1. Online attacks
2. Offline attacks
3. Non-electronic attacks

2.2.1 Online attacks of password cracking

- An attacker may create a **script- automated program-** to try each password
- Most popular online attack;- **man-in-the-middle attack or bucket-brigade attack**
- An attacker establish a **connection between victim and server.**
- Used to obtain passwords for **E-mail accounts** on public websites like gmail, yahoomail
- Also to get passwords for **financial websites**

2.2.2 Offline attacks of password cracking

- Are performed from a location other than the target where these passwords reside or are used
- Require physical access to the computer and copying the password
- Types of Password cracking attack.
 - Dictionary attack
 - Hybrid attack
 - Brute force attack

2.2.3 Non-electronic attacks of password cracking

- Social engineering
- Shoulder surfing
- Dumpster diving

2.2.4 Manual password cracking

1. Find a valid user account such as an administrator or guest;
2. Create a list of possible passwords;
3. Rank the passwords from high to low probability;
4. Key in each password;
5. Try again until a successful password is found.

2.2.4 Manual password cracking

Passwords can be guessed sometimes with knowledge of the user's personal information. Example of guessable passwords include :

1. Blank (none);
2. The words like “password”, “passcode”, and “admin”.
3. Series of letters from keyboard “qwerty”
4. Users' name or login name.
5. Name of users' friend/relative/pet.
6. Users' birthplace or date of birth or a relative's or a friend.
7. User's vehicle number, office number, residence number or mobile number
8. Name of a celebrity who is to be idol.
9. Simple modification of one of the preceding.

2.3 Password cracking techniques

- Dictionary attack
- Brute force attack
- Rainbow table attack
- Guess
- Spidering
- Social Engineering approach
- Shoulder surfing attack

2.3.1 Dictionary attack

- This method involves the use of a wordlist to compare against user passwords.
- For example, name123, 123xyz, etc

2.3.2 Brute force attack

- Brute force attacks use algorithms that combine alpha-numeric characters and symbols to come up with passwords for the attack.
- For example, a password of the value “password” can also be tried as p@\$word using the brute force attack.

2.3.3 Rainbow table attack

- This method uses pre-computed hashes.
- Database - stores passwords as md5 hashes.
- Create another database that has md5 hashes of commonly used passwords.
- Compare the password hash we have against the stored hashes in the database.
- If a match is found, then we have the password.

2.3.4 Guess

- This method involves guessing.
- Passwords such as qwerty, password, admin, etc. are commonly used or set as default passwords.
- Not changed or if the user is careless when selecting passwords

2.3.5 Spidering

- Most organizations use passwords that contain company information.
- Spidering gathers information from these sources to come up with word lists.
- The word list is then used to perform dictionary and brute force attacks.

2.3.5 Social Engineering Approach

- The attacker could pose as an IT security tech person and simply ask for network access password, or could pose PA of manager.

2.3.6 Shoulder surfing attack

- You look into our friend's computer's keyboard as he/she is typing his/her password.

2.4 Password cracking tool

- John the Ripper
- Cain & Abel
- Ophcrack
- L0phtCrack
- THC- Hydra

2.4.1 John the Ripper

- Uses the command prompt to crack passwords.
- Suitable for advanced users
- It uses to wordlist
- The program is free, but the word list has to be bought.
- It has free alternative word lists that you can use.
- Visit the product website <https://www.openwall.com/john/> for more information and how to use it.

2.4.2 Cain & Abel

- Runs on windows.
- Used to recover passwords for user accounts, recovery of Microsoft Access passwords; networking sniffing, etc.
- Uses a graphic user interface.
- Common among newbies and script kiddies
- Visit the product website <http://www.softpedia.com/get/Security/Decryption-Decoding/Cain-and-Abel.shtml> for more information and how to use it.

2.4.3 Ophcrack

- Cross-platform Windows password cracker - rainbow tables to crack passwords.
- It runs on Windows, [Linux](#) and Mac OS.
- It also has a module for brute force attacks among other features.
- Visit the product website <http://ophcrack.sourceforge.net/> for more information and how to use it.

2.4.4 L0phtCrack

- Password recovery application
- Test password strength
- Recover lost Microsoft Windows passwords
- Techniques used - Dictionary attack, Brute force attack, Rainbow table attack

2.4.5 THC- Hydra

- Fast and flexible parallelized login cracker
- Supports numerous protocols to attack

2.5 Password Cracking Counter Measures

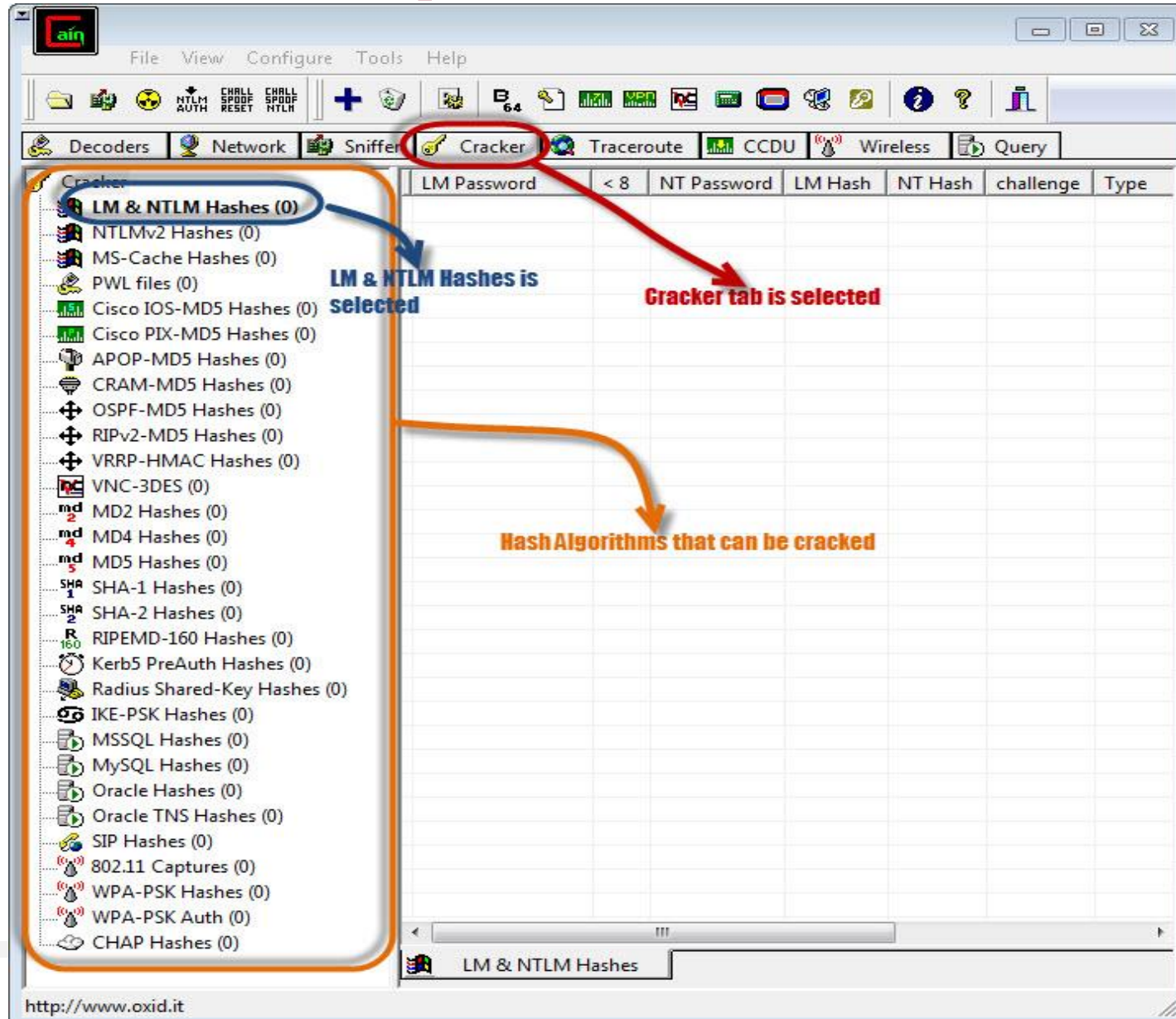
- Avoid short and easily predicable passwords
- Avoid using passwords with predictable patterns such as 11552266.
- Passwords stored in the database must always be encrypted.
- Organizations must adopt policies that favor high password strength numbers.

2.6 Hacking Activity: Password Cracking !

- Going to Crack Windows account with a simple password.
- Use the NTLM cracker tool in Cain and Abel to do that.
- Use the dictionary attack in this example.
- Need to download the dictionary attack wordlist here [10k-Most-Common.zip](#)
- For this demonstration, we have created an account called Accounts with the password **qwerty** on Windows 7.



2.6.1 Step for Password Cracking



- Open Cain and Abel, you will get such main screen
- Make sure the cracker tab is selected as shown

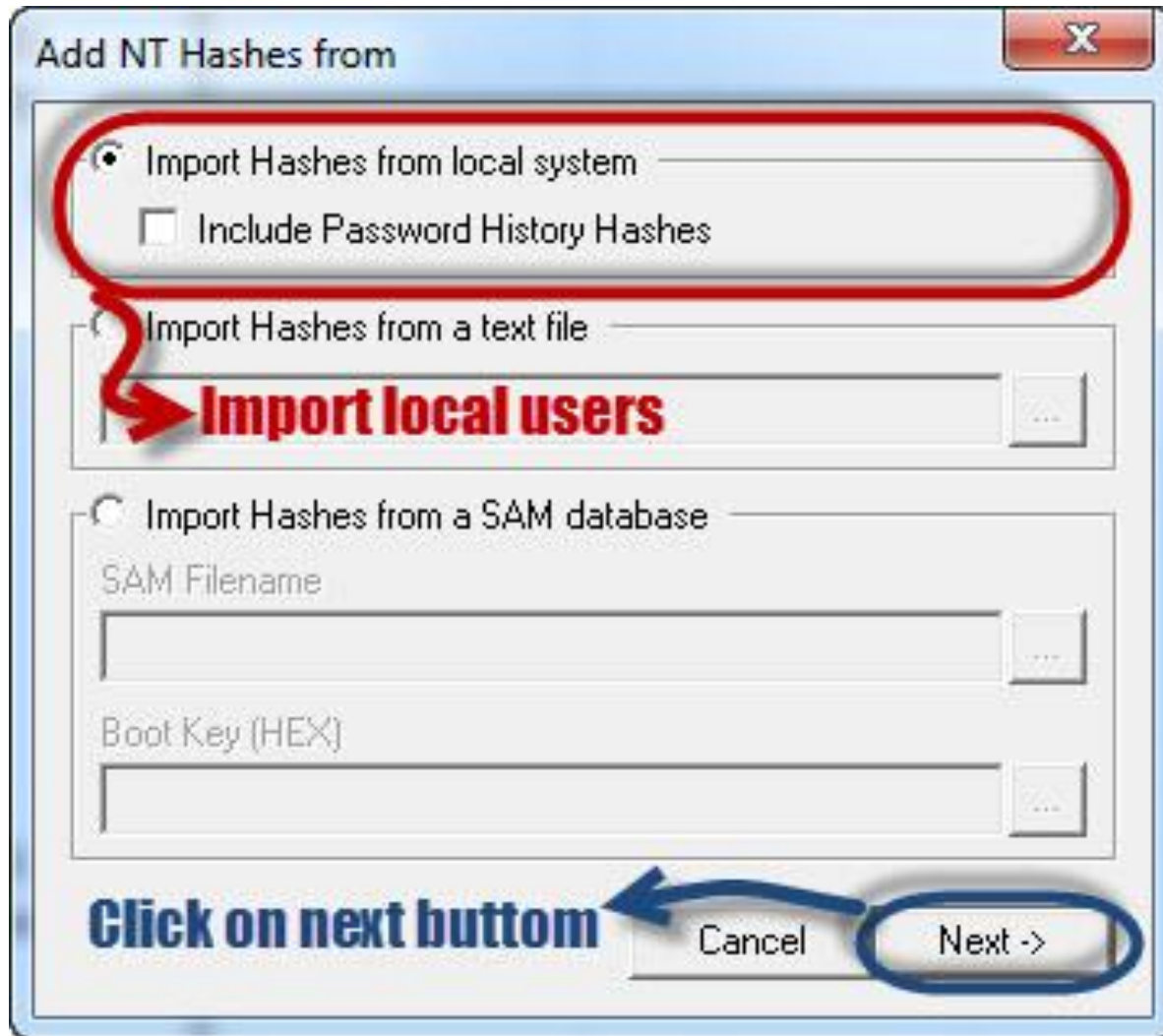
2.6.2 Step for Password Cracking



- Click on the Add button on the toolbar.

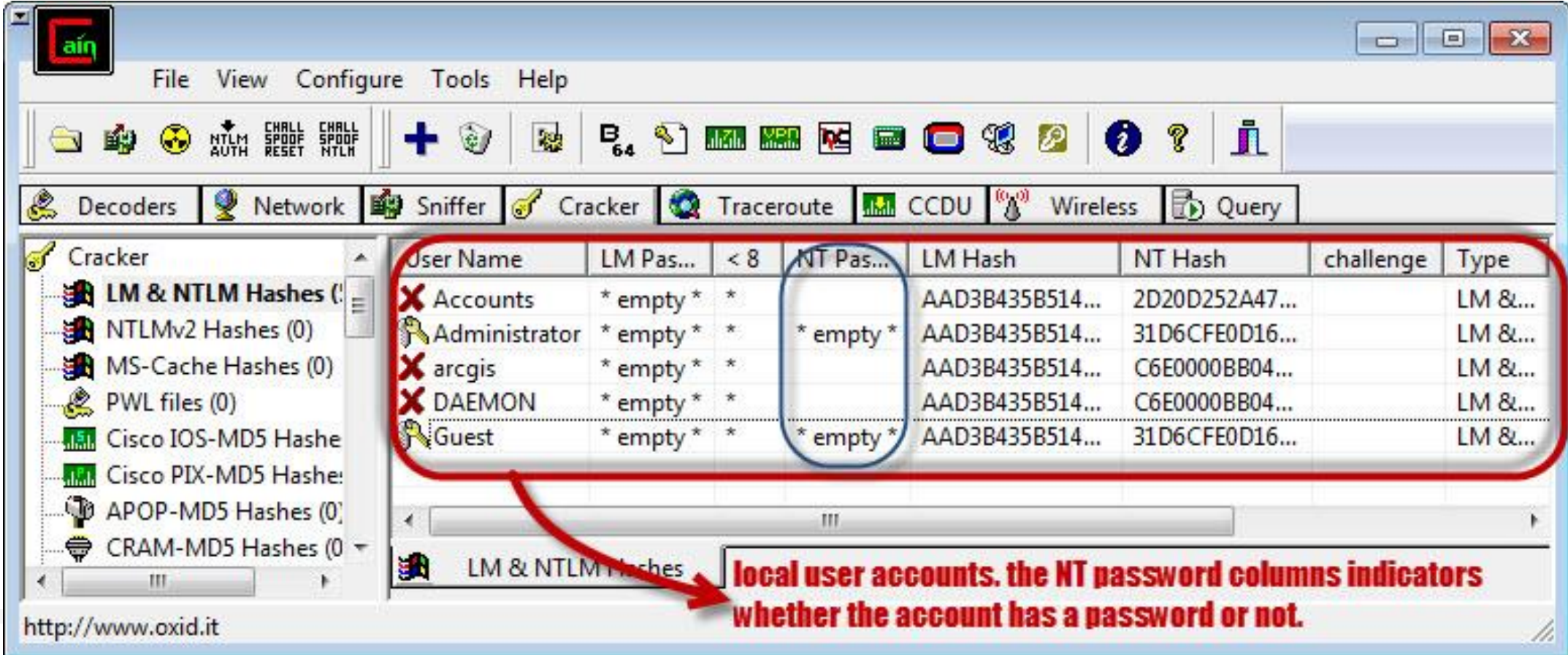
2.6.2 Step for Password Cracking

- Such dialog window will appear



2.6.3 Step for Password Cracking

- The local user accounts will be displayed as follows.
- Right click on the account you want to crack



The screenshot shows the main interface of Cain & Abel. The 'Cracker' tab is selected, displaying a table of local user accounts. The table has columns for User Name, LM Password, NT Password, LM Hash, NT Hash, challenge, and Type. The 'NT Password' column contains indicators: an 'X' for accounts without a password and a key icon for accounts with a password. A red box highlights the table, and a red arrow points from the 'NT Password' column to a text box at the bottom right.

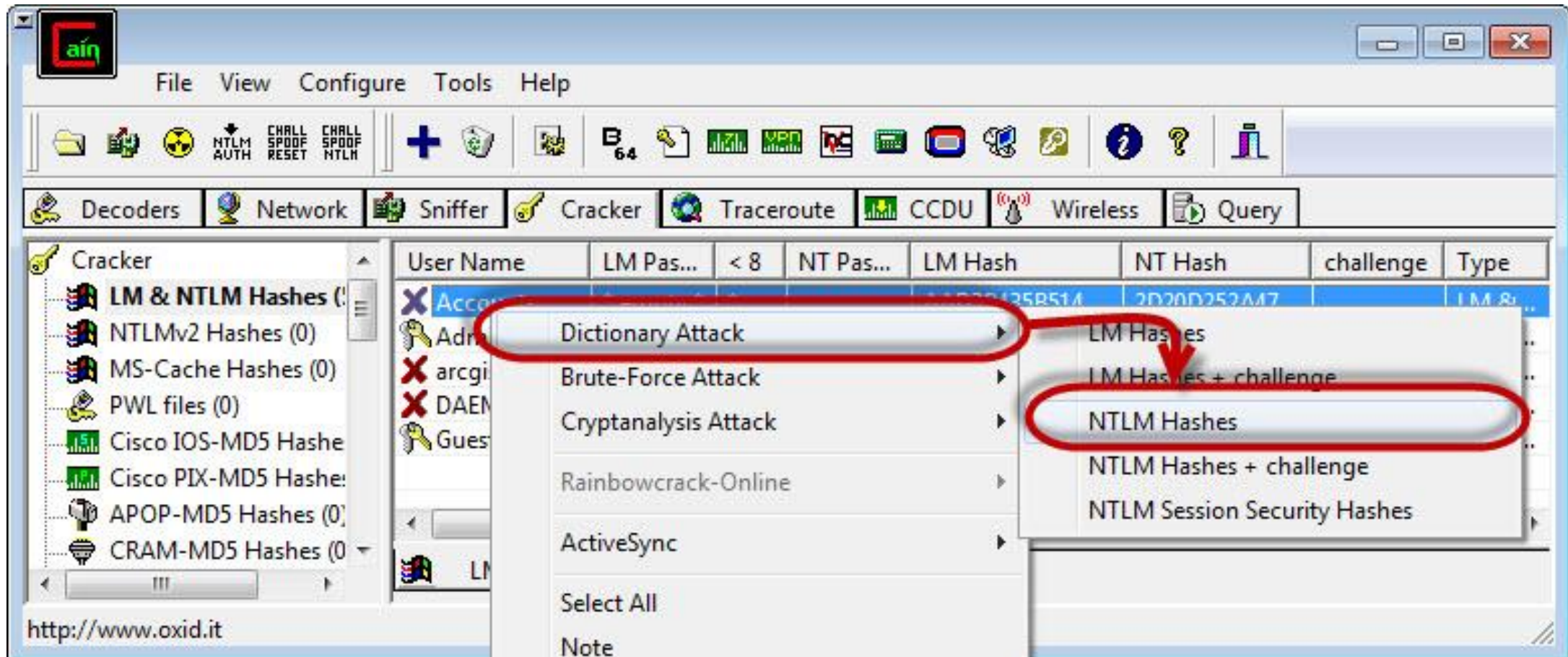
User Name	LM Pas...	< 8	NT Pas...	LM Hash	NT Hash	challenge	Type
Accounts	* empty *	*	X	AAD3B435B514...	2D20D252A47...		LM &...
Administrator	* empty *	*	Key	AAD3B435B514...	31D6CFE0D16...		LM &...
arcgis	* empty *	*	X	AAD3B435B514...	C6E0000BB04...		LM &...
DAEMON	* empty *	*	X	AAD3B435B514...	C6E0000BB04...		LM &...
Guest	* empty *	*	Key	AAD3B435B514...	31D6CFE0D16...		LM &...

local user accounts. the NT password columns indicators whether the account has a password or not.

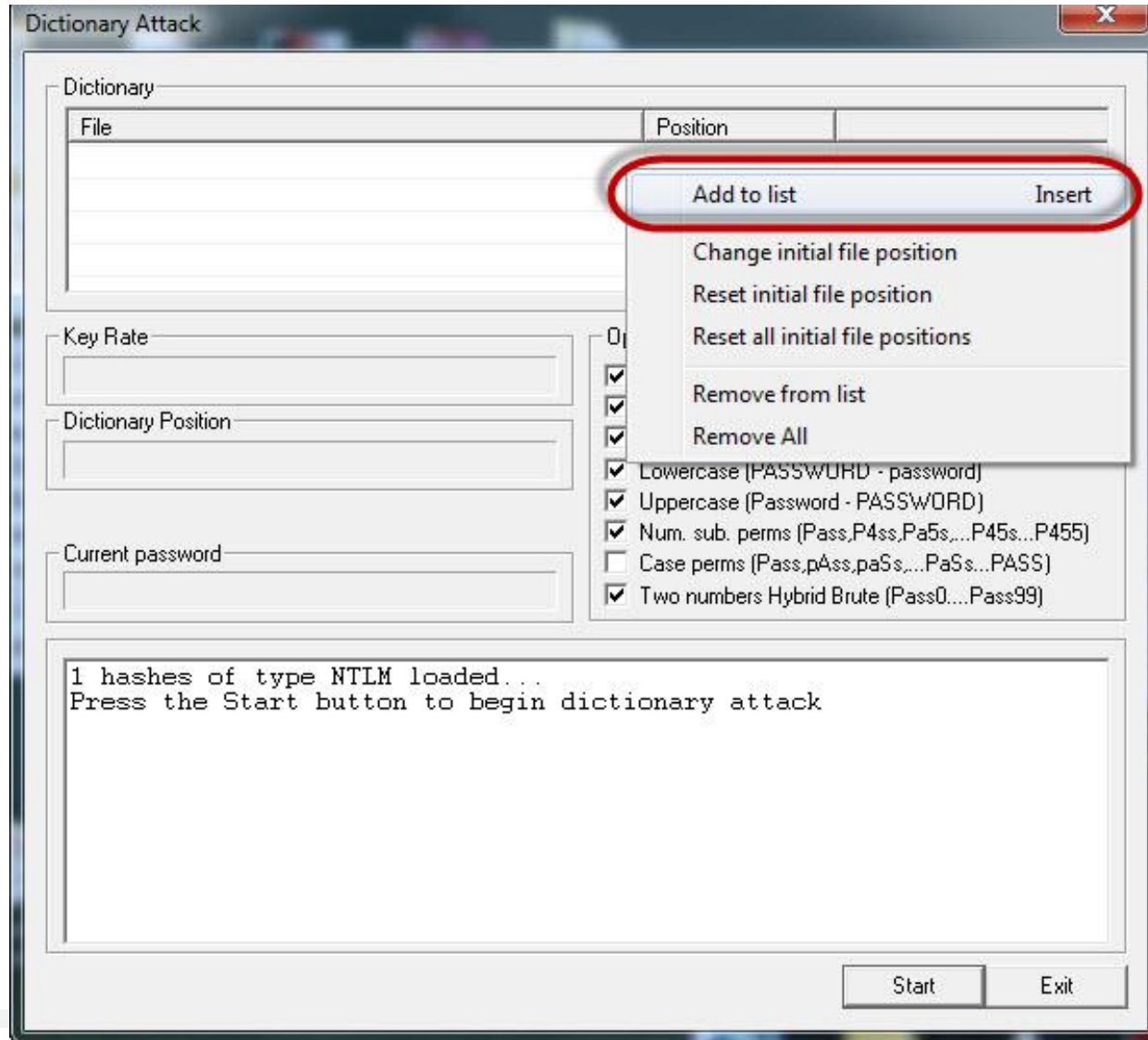
<http://www.oxid.it>

2.6.4 Step for Password Cracking

- The following screen will appear.

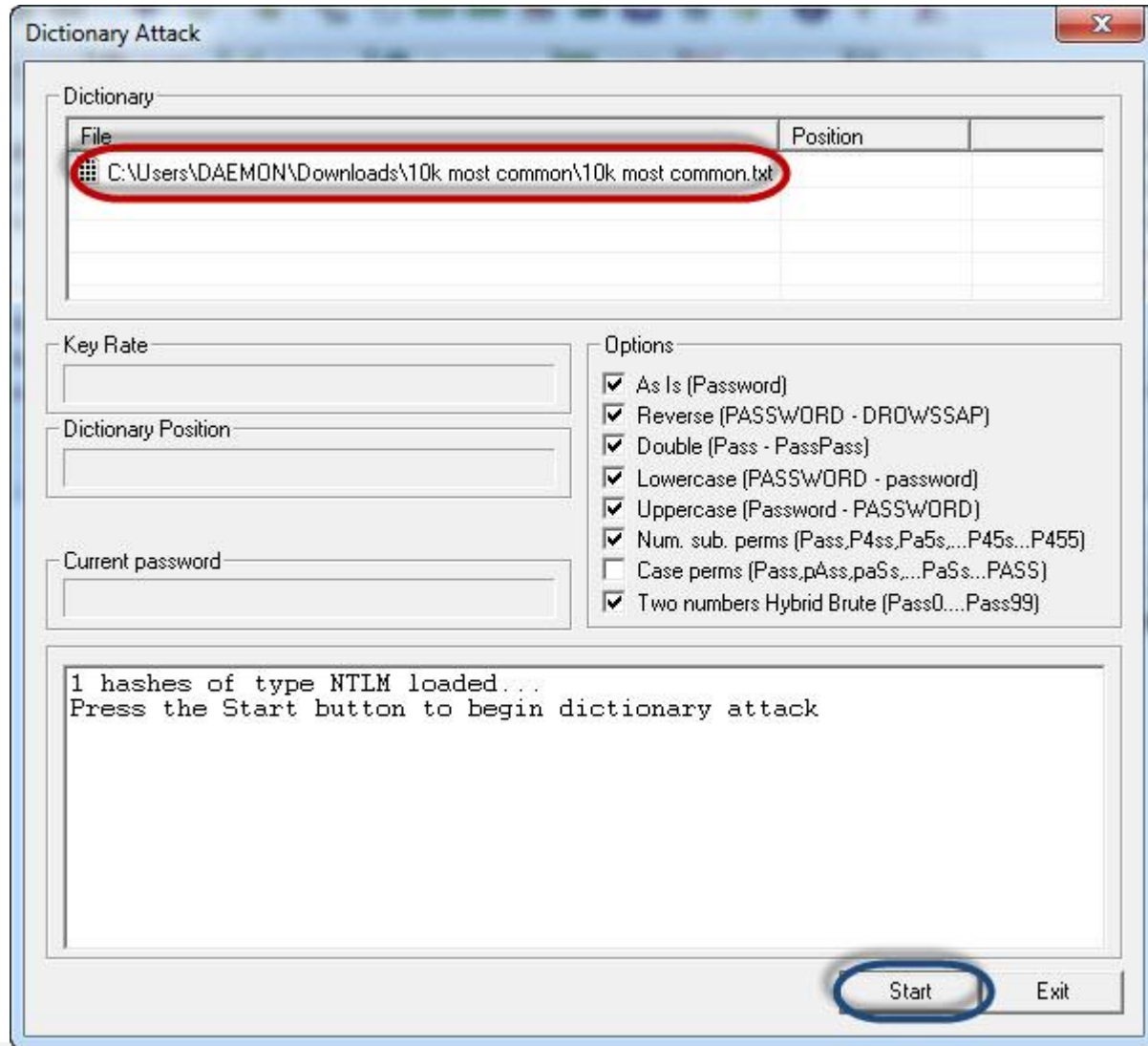


2.6.5 Step for Password Cracking



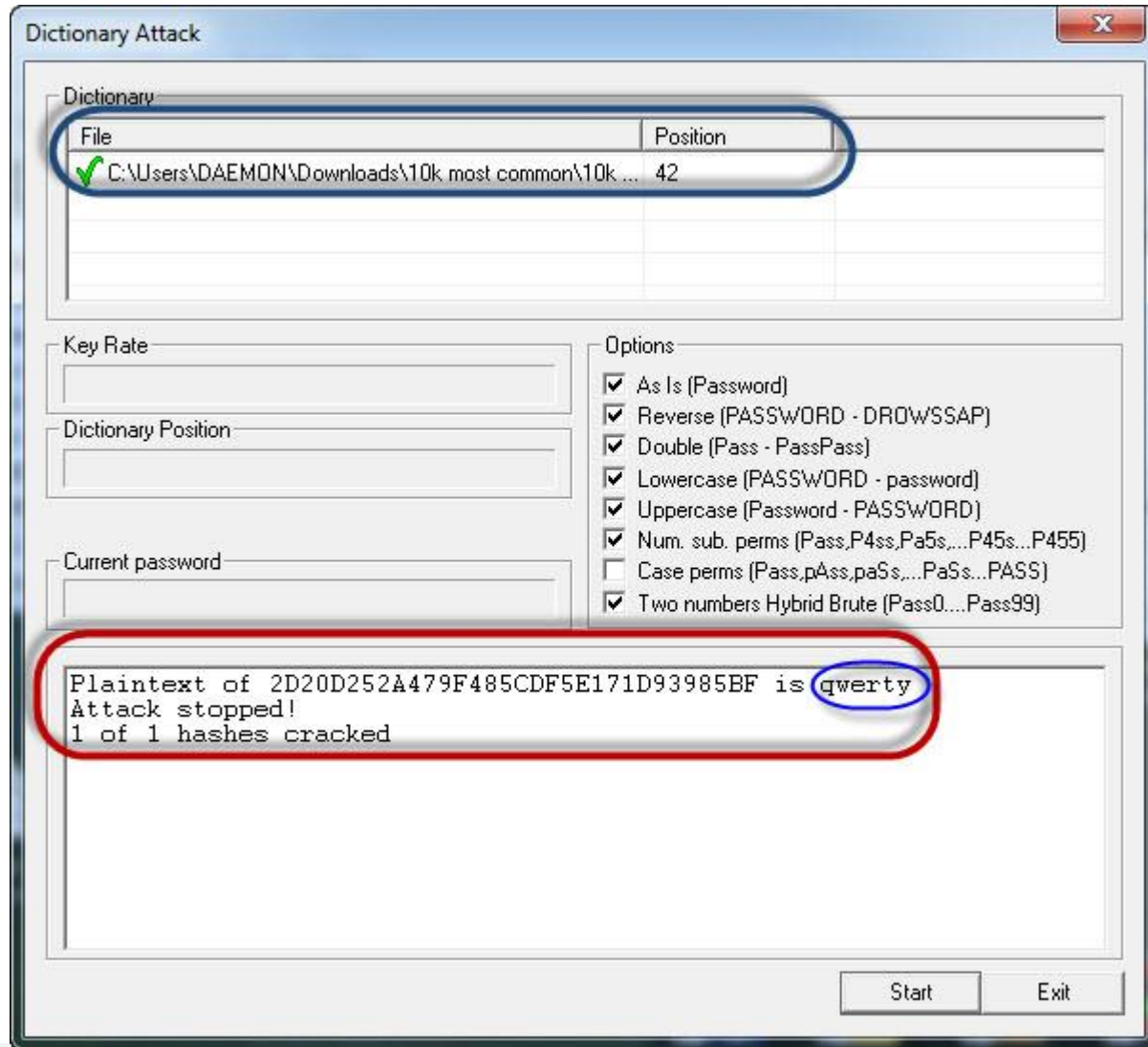
- Right click on the dictionary section and select Add to list menu as shown above

2.6.6 Step for Password Cracking



- Browse to the 10k most common.txt file that you just downloaded
- Click on start button

2.6.7 Step for Password Cracking



- If the user used a simple password like qwerty, then you should be able to get the following results.

2.7 Summary for Password Cracking

- The art of recovering stored or transmitted passwords.
- Password strength is determined - length, complexity, and unpredictability of a password value.
- Common password techniques include dictionary attacks, brute force, rainbow tables, spidering and cracking.
- Password cracking tools simplify the process of cracking passwords.

3. Keyloggers



3.1 Keyloggers



- Keylogger stores the key entered by user.
- It is most easy way to capture the password.
- Keylogger is a software or tools install remotely on system through viruses or Trojans.

3.2 How hackers use keyloggers ?

- The first keyloggers were used by the Soviet Union in the 1970s
- Today keystroke loggers are a common part of the cyber-criminal toolset to capture financial information such as banking and credit card details, personal information
- They may sell that information or use it as part of a larger attack
- Used to steal information like passwords, PII [personally identifiable information], and other critical information

3.3 Software keyloggers

- Software-based keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware and every keystroke is recorded
- They are installed on system using trojans or viruses
- Usually computers available on public places are infected
- Usually consists of two files DLL and EXE

3.3 Software keyloggers

- SC – KeyLog PRO
- Stealth keylogger
- KGB Spy
- SpyBuddy
- Elite keylogger

3.4 Hardware keyloggers

- Hardware based keyloggers can monitor your activities without any software being installed at all.
- Keyboard hardware
- Wireless keyboard sniffers
- Keyboard overlays

3.5 Acoustic keylogging

- Acoustic keylogging monitors the sound created by each individual keystroke and uses the subtly different acoustic signature that each key emits to analyze and determine what the target computer's user is typing.

3.6 Anti-Keylogger

- An **anti-keylogger** (or **anti-keystroke logger**) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on your computer.

3.6 Anti-Keylogger

- It detect the keylogger install in system.
- Advantage of anti-keylogger are listed as below.
 - Firewall can not detect the installation of keylogger on the system but anti-keylogger does it.
 - Anti-keylogger does not required regular updates.
 - It prevent internet banking fraud.
 - It prevent ID theft.
 - It secure E mail and internet messaging /chating.

3.6 Benefits of Anti-Keylogger

- **Keylogger removal** – It removes keyloggers that are running or being launched in your computer or mobile.
- **Security** – It ensures us that confidential information would not be stolen from our hard drives or computer units, and, prevents us from being a victim of cyber crimes and thefts. Financial institutions are usually targets of keyloggers. Anti-loggers perform regular scans in any computer.
- **Keylogger detector** – Apart from the “disabling” feature, the anti-keylogger provides a warning whenever a key logging activity is being launched in your unit.
- **Protects privacy** – As stated in reviews, it prevents your data or activities from being revealed through these keyloggers. Your messages, calls, videos, downloaded files, emails, website visits and other online transactions remain private unless you would reveal them yourself.
- **User friendly and reliable** – The anti-keylogger is easy to use and highly reliable

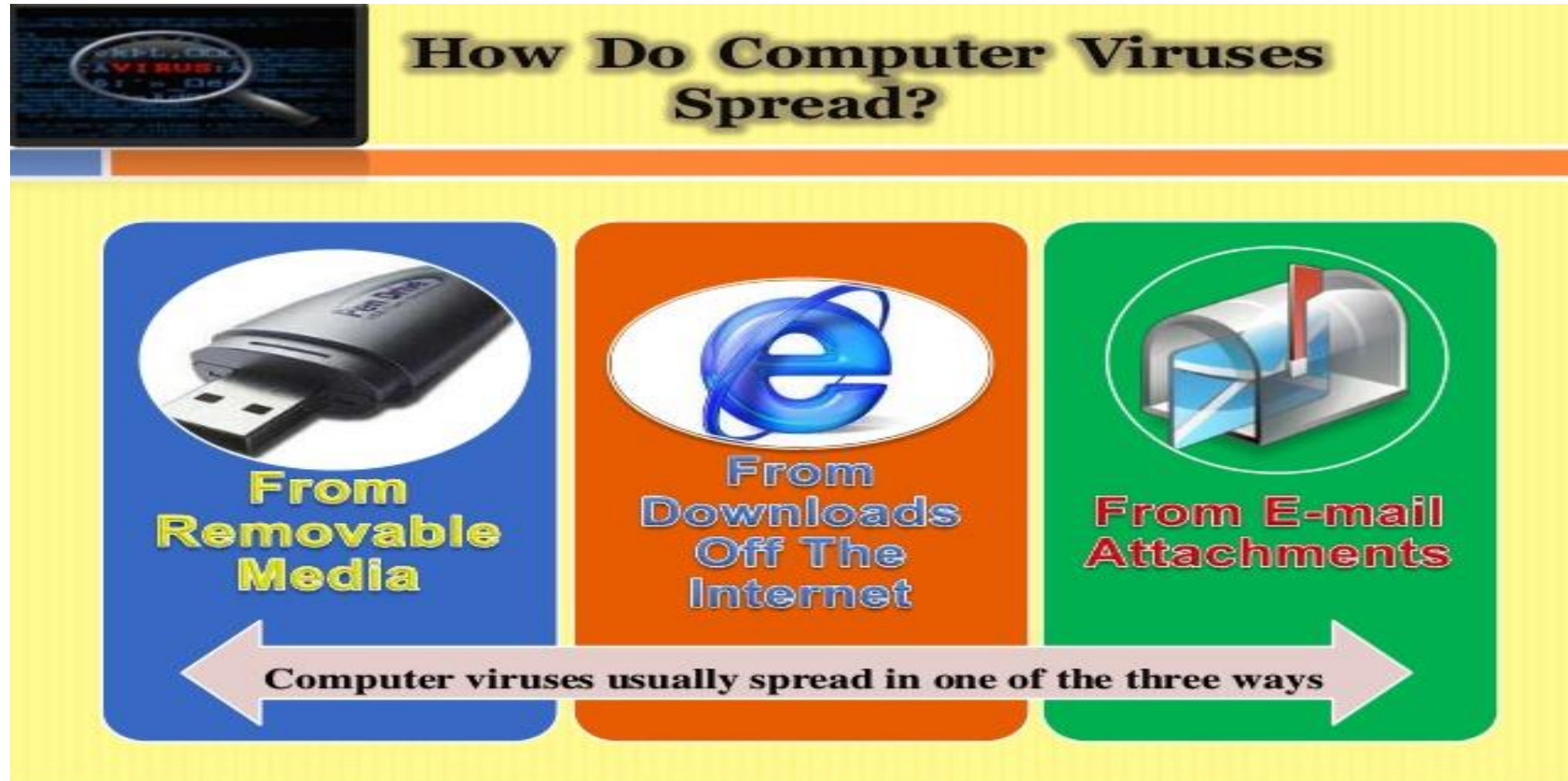
4. Spyware

- Spyware is malware (malicious software) which install on system and collect information about user without their knowledge.
- Spyware also collect information such internet surfing habits /pattern and website visited.
- Spyware will change computer internal setting.

4. Spyware Examples

- **007-Spy** : It has following feature
 - <http://www.e-spy-software.com> (007 Spy)
 - Override on antispay program like “Ad-aware”
 - record all web site URL
 - Powerful keylogger engine to capture all password.
 - It can view logs remotely from anywhere at anytime.
- Spector Pro : (<http://www.spectorsoft.com>)
 - Captures and reviews all chats and instant messages.
 - Capture E mail
 - Capture websites visited.
 - Capture activities perform on social networking sites

5. Virus and Worms



5.1 Virus

- A computer virus is a **malware** program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "**infected**".

5.1 Virus

Some typical virus actions :

- Display a message to prompt an action
- Delete files in the system
- Scramble data on a hard disk
- Cause erratic screen behavior
- Halt the system
- Replicate themselves to propagate further harm

5.1 Virus

Virus spread through

- The internet
- A stand alone PC
- Local networks

5.2 Types of Virus

- Boot sector virus
- Program virus
- Multipartite virus
- Stealth virus
- Polymorphic virus
- Macrovirus

Boot sector virus

- A boot sector virus is a computer virus that infects a storage device's master boot record (MBR).
- These viruses copy their infected code either to the floppy disk's boot sector or to the hard disk's partition table.
- During start-up, the virus gets loaded to the computer's memory.
- The propagation of boot sector viruses has become very rare since the decline of floppy disks.

Program virus

- A program virus becomes active when the program file (usually with extensions .BIN, .COM, .EXE, .OVL, .DRV) carrying the virus is opened.
- Once active, the virus will make copies of itself and will infect other programs on the computer.

Multipartite virus

- A multipartite virus is a fast-moving virus that uses file infectors or boot infectors to attack the boot sector and executable files simultaneously.
- The multipartite virus can affect both the boot sector and the program files at the same time, thus causing more damage than any other kind of virus.
- A multipartite virus infects computer systems multiple times and at different times.
- A multipartite virus is also known as a hybrid virus.

Stealth virus

- A stealth virus is a hidden computer virus that attacks operating system processes and averts typical anti-virus or anti-malware scans.
- Stealth virus eradication requires advanced anti-virus software or a clean system reboot.

Polymorphic viruses

- It is a self-encrypted virus designed to avoid detection by a scanner.
- Upon infection, the polymorphic virus duplicates itself by creating usable, slightly modified, copies of itself.
- In order for scanners to detect this type of virus, brute-force programs must be written to combat and detect the polymorphic virus with novel variant configurations.

Macro viruses

- A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.

5.3 Worm

- A Malicious program that keep making copies of itself on the local rive network shares, etc
- Keep preparing clones of itself
- Does not harm any data or file on computer
- Spreads by exploiting vulnerabilities in operating systems

5.4 Properties of Worm

- Infected machine becomes launching pad for attack
- Exploit software vulnerabilities
- Cause n/w connection to spread from system to system
- Spread through shared media
- May replicate
- Email worms spread in codes included in attachments and instant message transfer

5.5 Difference between virus and worm

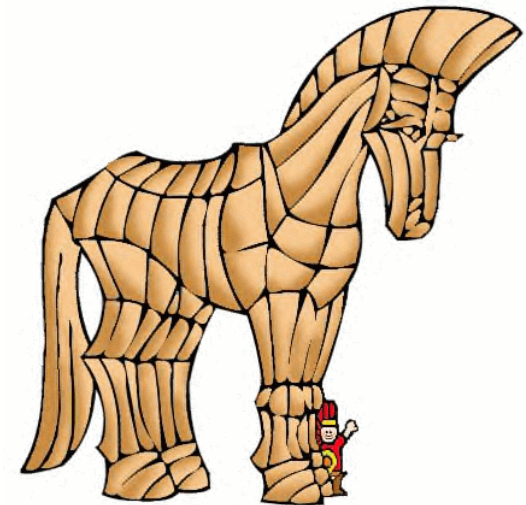
	Computer Virus	Computer Worm
How does it infect a computer system?	It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.
How can it spread?	It has to rely on users transferring infected files/programs to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.
Does it infect files?	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.
whose speed is more?	virus is slower than worm.	worm is faster than virus. E.g.The code red worm affected 3 lack PCs in just 14 Hrs.
Definition	The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.

5.6 Some of top Virus and Worm attacks

- Concept Virus
- CIH
- Melissa Virus
- Morris Virus
- ILOVEYOU
- Blaster Worm
- Code Red
- Storm Worm
- NimdaWorm

6.1 Trojan Horse

- Trojan horse is a program in which malicious or harmful code contain inside harmless programming or data.
- Trojan can insert into system in number of ways including web browser ,E mail, s/w downloadable from internet.
- Unlike virus and worms, trojan can not create multiple copy of itself , but it is equally destructive like virus and worms.
- Ex. waterfall.src screen saver.
- List of trojan horse is available on site
http://en.wikipedia/wiki/List_of_trojan_horses



6.1 Trojan Horse

Examples of threats by trojans

- Erase, overwrite or corrupt data on a computer
- Help to spread other malware such as viruses- dropper trojan
- Deactivate or interface with antivirus and firewall programs
- Allow remote access to your computer- remote access trojan
- Upload and download files
- Gather E-mail address and use for spam
- Log keystrokes to steal information – pwds, CC numbers
- Copy fake links to false websites
- slowdown, restart or shutdown the system
- Disable task manager
- Disable the control panel

6. Trojan Horse

Classification of trojans

- Remote access trojan
- Data sending trojan
- Destructive trojan
- Proxy trojan
- FTP trojan
- Security software disabler trojan
- DOS attack trojan
- Backdoor trojan
- Exploit
- Rootkits
- Trojan bankers
- Trojan downloaders

6.2 Backdoors.

- A backdoor is a means of access to a computer that bypasses security mechanism.
- Programmer or S/W developer install backdoor for troubleshooting or debugging purpose.
- A Backdoor work in background and hide from the user.



6.2 Backdoors.

Functions of backdoors

Allows an attacker to

- create, delete, rename, copy or edit any file
- Execute commands to change system settings
- Run, control and terminate applications
- Install software and parasites
- Control computer hardware devices
- Shutdown or restart computer

6.2 Backdoors.

Functions of backdoors

- Steals sensitive personal information, valuable documents, passwords, login name
- Records keystrokes, captures screenshots
- Sends gathered data to predefined E-mail addresses
- Infects files, corrupts installed apps, damages entire system
- Distributes infected files to remote computers
- Degrades internet connection and overall system performance
- Decreases system security
- Provides no uninstall feature, hides processes, files and other objects

6.2 Examples of Backdoors.

- **Back Orifice** : for remote system administration
- **Bifrost** : can infect Win95 through Vista, execute arbitrary code
- **SAP backdoors** : infects SAP business objects
- **Onapsis Bizploit**: Onapsis Bizploit is an SAP penetration testing framework

6.3 Trojan Horse and Backdoor

How to protect from Trojan Horse and Backdoor

- Stay away from suspect websites/weblink.
- Surf on the Web cautiously.
- Install antivirus /Trojan remover software.

Protection against viruses, worms, trojans and malware

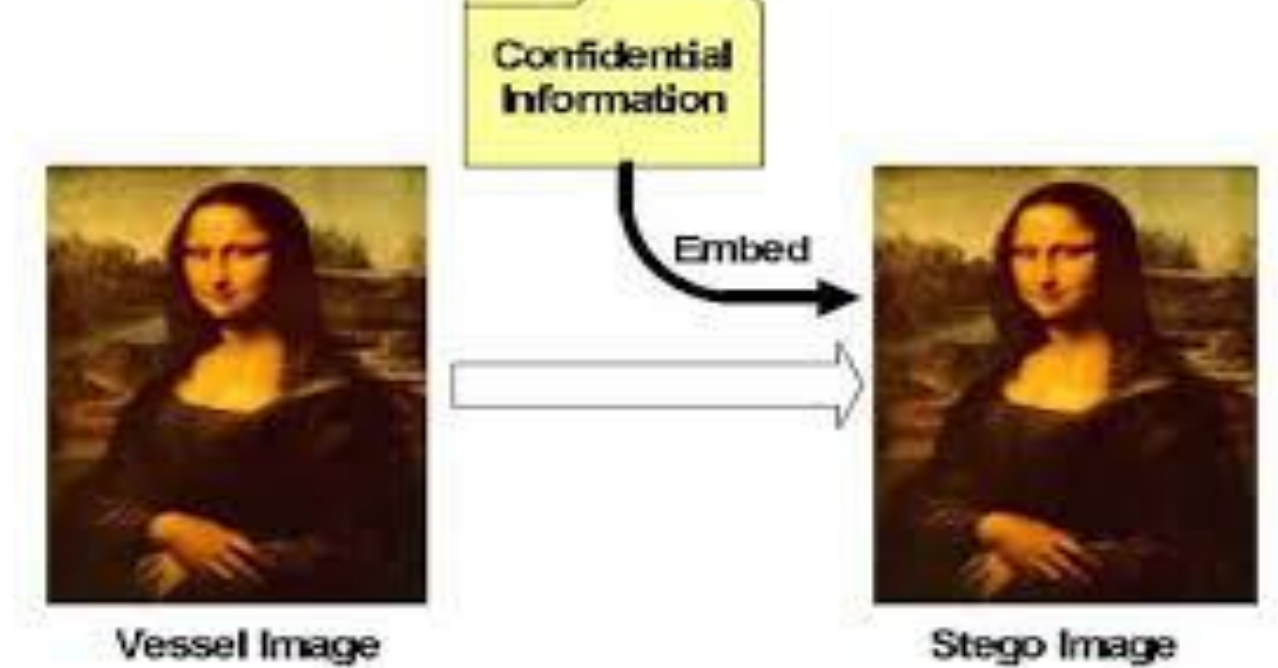
- Get a good anti virus
- Know what malicious program look like
- Be wary of email attachments
- Avoid third party downloads
- Have a hardware- based firewall
- Avoid Autorun
- Regularly back up your data

7. Steganography

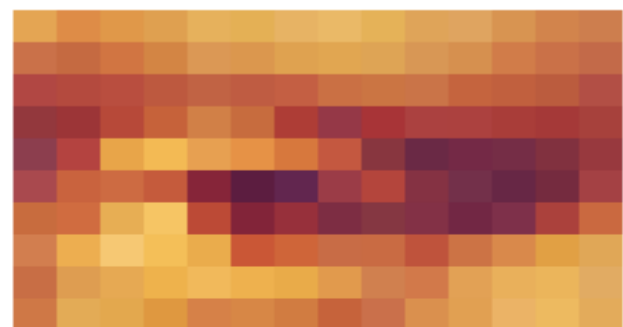
- Steganography (from Greek steganos, or "covered," and graphie, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination.
- Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.
- Other names: data hiding, information hiding, digital watermarking

7. Steganography

- Types of Steganography
 - Image Steganography
 - Audio Steganography
 - Video Steganography
 - Text Steganography



ORIGINAL IMAGE



R202 G212 B75
 R198 G99 B59
 R209 G124 B65
 R215 G135 B70
 R214 G129 B72
 R223 G152 B64
 R227 G168 B78
 R227 G171 B86
 R207 G120 B70

IMAGE WITH HIDDEN DATA



R203 G113 B75
 R198 G98 B58
 R208 G126 B67
 R215 G134 B70
 R215 G129 B75
 R223 G153 B67
 R226 G168 B81
 R226 G170 B88
 R206 G120 B71

Cryptography

- **Purpose:** Cryptography is like a secret code that helps protect information from unauthorized access. It's like putting your message in a locked box so that only the person with the key can read it.
- **Technique:** It uses complex mathematical algorithms to scramble data into a form that's difficult to understand without the right "key" to decode it.
- **Example:** Think of it like writing a letter in a secret language that only you and your friend know, so others can't understand it even if they see it.

Cryptography

Steganography

- **Purpose:** Steganography is like hiding something in plain sight. It's a way to hide information within other information, so it's not obvious that there's a secret message.
- **Technique:** Instead of changing the data, steganography embeds the secret information within another file, like an image or audio, making it hard to detect.
- **Example:** Imagine writing a secret message on a piece of paper and then covering it with a regular-looking drawing. To most people, it's just a drawing, but your friend knows where to find the hidden message.

Steganography

Watermarking

- **Purpose:** Watermarking is like adding a visible or invisible mark on something to show ownership or authenticity. It's often used to protect photos, documents, or videos from unauthorized use or copying.
- **Technique:** It involves adding a unique mark or pattern to the content. In digital media, it can be a faint logo or text that's overlaid on an image or video.
- **Example:** When you see a logo or text on a photo that says "Copyright © [Your Name]," that's a watermark. It tells people that the photo belongs to you, and they can't use it without your permission

Digital watermarking

- Digital watermarking is the act of hiding a message (trademark) related to a digital signal (i.e. an image, song, video) within the signal itself.
- Watermarking tries to hide a message related to the actual content of the digital signal
- while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Difference between steganography and *cryptography*

- Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists.
- In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world.
- Due to this, Steganography removes the unwanted attention coming to the hidden message.
- Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content.
- By combining Steganography and Cryptography one can achieve better security.

Difference between *cryptography*, steganography and watermarking

	1	2	3
	Cryptography	Steganography	Watermarking
Definition	is the art and science of secret writing	is the art and science of hiding information	is the process of embedding a message on a host signal
secret message	is unreadable, understandable, opaque and data is scrambled	is imperceptible, data is hidden and isn't scrambled	is Inviavle or perceptual visible depending on the requirement
objective	make the message unreadable to anyone who doesn't have the key and know the correct algorithm.	hide the existence of the message	marking media files with copyright information and avoid illegal copying
Security	No one would be able to know what the message says unless there's a key to the code	The hidden message is imperceptible to anyone	An unauthorized person cannot detect, retrieve or modify the embedded watermark

Steganalysis

- **Steganalysis** is the study of detecting messages hidden using steganography
- Example:
 - StegExpose
 - StegSecret

8. DoS and DDoS

In computing, a **denial-of-service (DoS)** or distributed **denial-of-service (DDoS) attack** is an attempt to make a machine or network resource unavailable to its intended users.

- Flood the bandwidth of victim network.
- Flood the resources of the system.
- Flood the victim E-mail box with spam mail.
 - IP Spoofing (Forge IP address) tech is use to flood victim machine.

How to perform a DoS/DDoS attack

https://www.youtube.com/watch?v=fGWkhmCp_js

Symptoms of DoS attacks

- Slow network performance
- Unavailability of a particular website
- Inability to access any website
- Dramatic increase in number of Spam E-mails received

A DoS attack may do the following

- Flood the traffic, thereby preventing network traffic
- Disrupt connections between two systems- preventing access to service
- Prevent a particular individual from accessing a service
- Disrupt service to a specific system or person

Classification of DoS

- Bandwidth attacks
- Logic attacks
- Protocol attacks
- Unintentional DoS attack

Tools used to launch dos/ddos attacks

- Trinoo
- TFN
- TFN2K
- Stacheldraht

How to prevent dos/ddos attacks

- Buy more BW
- Build redundancy in your architecture
- Configure you network hardware
- Deploy anti DOS hardware and software modules
- Deply DDOS Protection appliance

Protection from DoS and DDoS

- Implement router filter. Filter will help to minimize DoS attack.
- Install patches to guard system against TCP SYN flooding.
- Disable any unseen network services.
- Decide normal and abnormal activity of system.
- Routinely exam physical security of system.
- Identified redundant and fault tolerant network configuration.
- Take regular backup of system.

Tools for Detecting DoS/DDoS attack.

- **Zombie Zapper** : This tool instruct Zombies to stop flooding .
- **Remote Intrusion Detection (RID)** : It is packet snooper and generator.
 - Snooper : It is a spy who makes uninvited inquiries into the private affairs of others.
 - It send packet in the form of config.txt and then listening appropriate replies.
- **Find _DDoS** : This tool scan system to detect DDoS attack.
- **DDoSPing** : It is remote network scanner .
It detect Trinoo, Tribe Flood with their default seating.

Sql Injection



Sql Injection

- SQL is used to define database , update database and retrieve information from database.
- Sql injection is result of vulnerability present at database layer.
- The vulnerability is exposed when user entered string **escape char** embedded in sql statement.
- SQL injection is a example of such vulnerability where one scripting lang. is embedded inside another.
- Attacker will target of database which store confidential information. (password , Credit card no, debit card no).

Steps for SQL Injection

1. Attacker will search for web page (UI) .
2. Attacker can view the source code of the script through **source view** option of IE (Internet Explorer). In source code ,attacker will search for <FORM> </FORM> tag.
3. This tag contain parameter that might useful to find vulnerability.
4. The attacker inputs a single quote in text box of web page to accept username and password.
5. Attacker enter following variable on web page to test for sql vulnerability.

Blah' or 1=1-;

login.blah or 1=1-;

Password :: blah' or 1=1--;

http://search/index.asp ? id blah' or 1=1--

Blind Sql Injection

- Blind SQL injection is used when web application is vulnerable to an SQL injection but result of the injection are not visible to the attacker.
- In summery SQL injection attacker can,
 1. Obtain basic information
 2. May gain access to the system by obtaining username and password.

select * from user where name="OR '1'='1'."

3. Add new data to the dataset. (insert command)
4. Modify data currently in the database. (update command)

SQL Injection :

<https://www.youtube.com/watch?v=uSw0IoSr3Hkl> Injection attack

Tools used for SQL server penetration

- AppDetectivePro : This tool access database application and their security strength within network.
- DbProtector : This tool is responsible for
 - Database asset management.
 - Vulnerability management.
 - Audit and threat management.
 - Policy management.
 - reporting and analysis.
- Database scanner : Offers security policy generation and reporting functionality which instantly measures policies and automates the process of security

How to prevent SQL Injection Attack

- Sql injection is result of poor website administration and coding.
- Prevention mechanism ,

1. Input Validation.

- Replaces all single (escape quotes)quotes to two single quotes.
- Check input.
- Check numeric value using IsNumeric() function.
- Keep proper size of text box and input box.
- Sql error should not display to outside the user.

How to prevent SQL Injection Attack

2. Modify error reports- SQL errors should not be displayed to outside users. The developers should handle and configure the error reports very carefully
3. Other preventions
 - Do not use default setting for SQL server 2000.
 - Isolate database and web server.
 - Attacker are using stored procedure `xp_cmdshell ()`, `xp_grantlogin()` in SQL injection attack.

Title: Assignment based on Tools used in cyber security

Module -3: Tools and Methods Used in Cyber line

Exploring the vast landscape of cybersecurity tools reveals a complex ecosystem. List the key functionality, significance, and real-world application of a specific cybersecurity tool of your choice, and how does it contribute to the ongoing efforts to protect digital assets and information in an increasingly interconnected and vulnerable world?

Buffer Overflow

- C compiler does not check buffer overflow.

```
int main( )  
{  
    int buffer[10];  
    buffer[20]=10;  
}
```

Buffer Overflow

Types of Buffer overflow

In software, a **stack buffer overflow** (also known as **stack smashing**) occurs when a program writes to a memory address on the program's call stack outside of the intended data structure; usually a fixed length buffer.

- This almost always results in corruption of adjacent data on the stack, and in cases where the overflow was triggered by mistake, will often cause the program to crash or operate incorrectly.
- "shellcode" starts with command shell from which the attacker can control the compromised machine

NOPs (No operation perform)

- NOP reserve space which will be replace by active instruction .
- Collection of NOP is called as NOP sled.
- A NOP-sled is the oldest and most widely known technique for successfully exploiting a stack buffer overflow.
- NOP allow user to find the exact address of the buffer.
- Attacker can pad his code with NOP operation.

Heap Buffer overflow

- A buffer overflow occurring in the heap data area is referred to as a heap overflow
- Memory on the heap is dynamically allocated by the application at run-time and typically contains program data.

How to minimize bufferoverflow

- Assessment of security code manually.
 - Buffer overflow is a result of storing more than capacity.
 - Developer should minimizing the use of c lib.
- Disable stack execution
 - Malicious code will try to provide input to program from stack segment rather than code segment.
- Compiler Tools :
 - It generates warning to user , if they uses gets(),strcpy().
- Dynamic runtime check
 - This techniques ensure that code should load in secured manner before execution.

Attack on wireless Network

- Wireless network consist two elements.
 - Wireless access point.
 - Wireless enabled device.

User may access wireless network through dongle.

Networking standard

802.11 - It is applicable to WLAN.

- It supports 1 or 2 mbps transmission.
- 2.4 GHz band using FHSS (freq hopping spread spectrum)

802.11 a - It provides 54 mbps transmission in 5 GHZ band.

- It uses OFDM (orthogonal freq. div. mult. tech . Which is better than FHSS)

- 802.11 b - it provides 11 mbps transmission in 2.4 GHz band.
 - It uses complementary code keying (CCK) modulation to improve speed.
- 802.11g - it provides 54 mbps transmission in 2.4 GHz band.
 - It uses OFDM.
- 802.11 n : - 802.11 n is providing 54 mbps transmission speed .
It can only achieve 24 mbps of speed due to n/w conj.

- 802.15 - This standard is used for personal WLAN and cover very short range. Here it is used for Bluetooth technology.
- 802.16 – It is also known as WiMax .
 - It combine the benefits broadband and wireless. It provide high speed internet over long distance.

This standard is developed by IEEE.

Ex. wireless MAN.

Access point : It is act as a communication HuB.

Wi-Fi Hot spot : A hotspot is a site that offers the internet access by using Wi-Fi technology over a WLAN.

- Hotspot are found in public area.

- SSID (Service Set Identifier) : All wireless devices must use same SSID to communicate with each other.
SSID is set WLAN setup.
SSID is 32 char long.
- Wired equivalent privacy (WEP) .
Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks
WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.

Methods of Phishing

1. Dragnet
2. Rod and reel
3. Lobsterpot
4. Gillnet

Phishing Techniques

1. URL manipulation
2. Filter evasion
3. Website forgery
4. Flash phishing
5. Social phishing
6. Phone phishing

Phishing related terms

- Homograph attack: two words are spelled in same way but differ in meaning
 - www.google.com--- www.g00gle.com
- Spear Phishing: Method of sending phishing message to a particular organization to gain organizational information
- Whaling: It may have been derived from the fact that people targeted are top ranking executives.

Phishing related terms

- Pharming: aimed to redirect a website's traffic to another bogus website
- Phoraging: process of collecting data from many different online sources to build up the identity of someone with ultimate aim of committing identity theft
- DNS hijacking: DNS redirection- DNS hijacker use malware in the form of a Trojan to exchange the legitimate DNS server assignment by ISP with a manual DNS server assignment from a bogus DNS server
- Click Fraud: An illegal practice that occurs when individuals click on a website through advertisements to increase the payable number of clicks by the advertiser

Types of Phishing

1. Deceptive Phishing
2. Malware based Phishing
3. Keyloggers
4. Session hijacking
5. In- session Phishing
6. Web trojans
7. Pharming
8. System reconfiguration attacks
9. Data theft
10. Content injection Phishing
11. Man in the middle Phishing
12. Search engine Phishing
13. SSL certificate Phishing

Phishing Countermeasures

1. Keep anti virus up to date
2. Do not click on hyper links in emails
3. Take advantage of anti spam software
4. Verify https
5. Use anti spyware software
6. Get educated
7. Firewall
8. Use Backup system images
9. Do not enter sensitive or financial information into pop up windows

Identity Theft

- Identity theft can be defined as the fraudulent use of someone else's identity to gain a financial advantage or obtain credit or other benefits in that person name.
- It is of types
 - True name
 - Account take over

Types of Identity theft

- Financial Identity theft
- Criminal Identity theft
- Medical Identity theft
- Insurance Identity theft
- Child Identity theft
- Synthetic Identity theft
- Business Identity theft

Techniques for Identity theft

- Dumpster diving
- Shoulder surfing
- Phishing and spam email
-

Steps to prevent Identity theft

- Check your credit card statement periodically
- Shred unsolicited credit card applications
- Monitor your account statements for any unauthorized transactions
- Follow up with creditors in case there are fraudulent transactions
- Do not respond to spam emails



Join CSL on MS Teams:

Team Name: EXTC_Sem7_CSL_HarshadaRajale

Code: gppoi8w



THANK YOU

....



HARSHADA ARUN RAJALE



+91 9594146413



Harshada.Rajale@vit.edu.in