Password Cracking :

- What is Password?
- Password Cracking Concepts
- Types of Password Attacks
- Application Software Password Cracking
- Hardening the password

What is Password

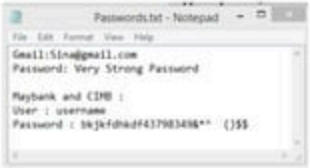
- String of characters for authentication and log on computer, web application , software, Files , network , Mobile phones, and your life ☺
- Comprises:

[a-zA-z, 0-9, symbols , space]

Password Characteristics

- No short length
- No birthday or phone number, real name , company name
- Don’t use complete words or Shakespeare quotes ☺
  - Example:
  - Hello123: Weak
  - @(H311l0)@: Strong
  - Easy to remember, hard to guess

Password Security



- Don’t use your old passwords
- Don’t use working or private email for every website registration such as games, news,….etc.

Password Cracking Concept

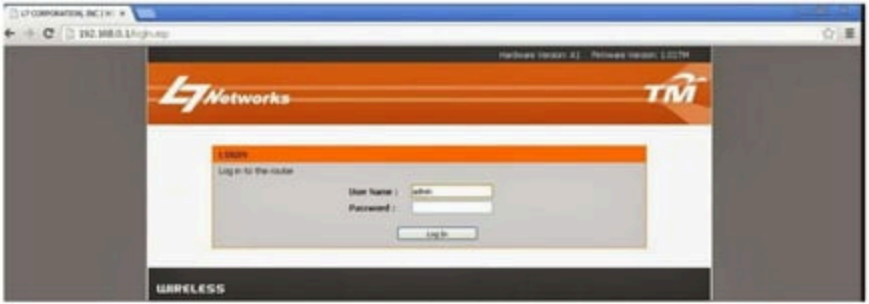
- guessing or recovering a password
- unauthorized access
- To recover a forgotten password
- A Penetration testing step (e.g. Network and Applications)

Type of Password Attacks

- Dictionary Attack
- Brute Force Attack
- Rainbow table attack
- Phishing
- Social Engineering
- Malware
- Offline cracking
- Guess

Password Cracking Types: (Guessing Technique)

I have tried many friends house and even some companies that , their password was remained as default, admin, admin ☺. *(Using Guessing Techniques)*



Password Cracking Types: (Phishing)

Password Cracking Types: (Social Engineering)

- sometimes very lazy genius non-IT Geeks can guess or find out your password

Password Cracking Tools

- **Brutus**

  Remote online cracking tool, Windows base, free, supports:(HTTP, POP3, FTP, SMB, ...etc), resume/pause option .no recent update but still on top ranking.

- **RainbowCrack**

  Hash cracker tool, windows/linux based, faster than traditional brute force attack, compare both plain text and hash pairs. Commercial and free version

- **Wfuzz**

  Web application brute forcing (GET and POST), checking (SQL, XSS, LDAP,etc) injection

- **Cain and Able *****

  Few features of password cracking ability: Syskey Decoder,VNC Password decoder , MS SQl MYSQL and Oracle password extractor Based64, Credential Manager Password Decoder, Dialup Password Decoder,PWL Cached Password Decoder, Rainbowcrack-online client, Hash Calculator,

- **John the Ripper**

  Offline mode, Unix/linux based, auto hash password type detector, powerful, contain several built-in password cracker

- **THC Hydra**

  Dictionary attack tool for many databases, over 30 protocols (e.g. FTP,HTTP,HTPPS,...etc)

- **Medusa**
- **AirCrack-NG**

  WEP and WPA-PSK keys cracking, faster than other WEP cracker tools

- **OphCrack**
- **L0phtCrack**

Password Cracking Types: (Offline Cracking)

- We have enough time to break the password
- Usually take place for big data
- Or very strong and complicated password
- After attack
- Forensics investigation

Password Hardening

- Techniques or technologies which put attacker, cracker or any other malicious user in difficulties
- Brings password policy
- Increase the level of web,network , application and physical access of to the company or organization.
- Using biometric technologies such as fingerprint, Eye Detection, RFID Tag Cards….etc
- All the Security solution just make it more difficulte. Harder but possible

Password Cracking Depends on

- Attacker's strengths
- Attacker's computing resources
- Attacker's knowledge
- Attacker's mode of access [physical or online]
- Strength of the passwords
- How often you change your passwords?
- How close are the old and new passwords?
- How long is your password?
- Have you used every possible combination: alphabets, numbers and special characters?
- How common are your letters, words, numbers or combination?
- Have you used strings followed by numbers or vice versa, instead of mixing them randomly?

Key logger and spyware

Define Key logger

Hardware Examples

Software Examples

Prevention

What is Keylogging?

Keystroke logging

A program or hardware device that captures every key depression on the computer

Used to monitor employee performance

Used to seal private information

Malicious Uses...

Besides being used for legitimate purposes, keyloggers can be hardware installed to a computer or software that is used to collect sensitive information.

The types of sensitive information include:

Usernames & Passwords

Credit Card Numbers

Person Information such as Name, Address, etc.

Keylogging Hardware...

These small devices connect directly on the end of a keyboard to the port on the computer and look rather unassuming.

At a later time the person who installed the keylogger can come back to retrieve it. They are easily removed.

Source:
http://epic.org/privacy/dv/keylogger_hw.gif

Software…

There are hundreds of keylogger programs available over the internet for download.

There are three ways for an attacker to install the software on an unsuspecting computer.

1. Install it from a compact disc or floppy disk.
2. Package the software as a computer virus or trojan horse.
3. Gain access to the computer over a network and install surveillance software remotely.

Viruses...

A simple search of a virus encyclopedia shows 500 examples of keylogging malware.

Prevention…

There are several ways to prevent Keyloggers:

- Anti-Virus/Spyware & Firewalls
- Automatic Form Fillers
- Alternative Keyboard Layouts
- On screen Keyboards

Anti-Virus/Spyware & Firewalls...

As with any Virus or Spyware you should make sure that you have up-to-date protection.

Anti-Virus:
Make sure its running and using the latest virus definitions.

Anti-Spyware:
Same as your Anti-Virus Software, update regularly.

Firewall:
Make sure its active. It's the first line of defense from online intrusions.

AutoForm Fillers…

A common feature of Web Browsers including Internet Explorer and Firefox.

Works against keyloggers but vulnerable to other security breaches.

Alternative Keyboard Layout...

Alternative keyboards make captured keystrokes look like nonsense

You can customize your own board with Microsoft Keyboard Layout Creator

On Screen Keyboards...

Software based keyboards are not very effective.

Clicks are converted back to keystrokes.

On Screen Keyboards...

Web-based Keyboards offer more protection and are often found in online games.

Summary…

Key Loggers record keystrokes:

- Legitimate use: Monitor employee productivity
- Illegal uses: Steal passwords, usernames, and other personal/corporate data

There are ways to protect yourself:

- Be aware of what's installed on your computer
- Use caution when surfing the internet
- Keep your computer's security software updated