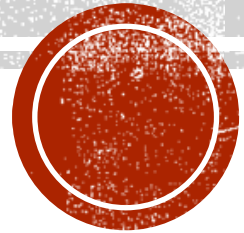
PASSWORD CRACKING



PASSWORD CRACKING

- Password Cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.
- The purpose of password cracking is as follows:
  - To recover a forgotten password.
  - As a preventive measure by system administrators to check for easily crackable passwords.
  - To gain unauthorized access to a system
- Manual password cracking is to attempt to logon with different passwords
- Passwords can be guessed sometimes with knowledge of the user's personal information.

CONT...

- The attacker follows the following steps:
  - Find a valid user account such as Administrator or Guest;
  - Create a list of possible passwords;
  - Rank the passwords from high to low probability;
  - Key-in each password;
  - Try again until a successful password is found.

EXAMPLES

- Blank(none);
- The words like “password”, ”passcode” and “admin”;
- Series of letters from the “QWERTY” keyboard, for example, qwerty, asdf or qwertyuiop;
- User’s name or login name;
- Names of user’s friend/relative/pet;
- User’s birthplace or date of birth, or a relative’s or a friend’s
- User’s vehicle number, office number, residence number or mobile number;
- Name of a celebrity is considered to be idol (eg: actor, actress, spritual gurus) by the user;
- Simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

CONT...

- An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list. This is considered manual cracking, but is time-consuming and not usually effective. Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource. To ensure confidentiality of passwords, the password verification data is usually not stored in a clear text format. When a user attempts to login to the system by entering the password, the same function is applied to the entered value and the result is compared with stored value. If they match, user gains the access; this process is called authentication.
- Some of the password cracking tools are :
  - 1.Cain and Abel
  - 2.Aircrack-ng
  - 3.L0phtcrack
  - 4.John the Ripper
  - 5.Pwdump 6.Brutus

TYPES OF PASSWORD CRACKING

- Password cracking attacks can be classified under three categories as follows:
  - 1. Online attacks
  - 2. Offline attacks
  - 3. Non-electronic attack
- Online attacks :
- An attacker can create a script file (automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system.
- The most popular online attack is man-in-the-middle (MITM) attack also termed as bucket-brigade attack.
- Man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
- This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also get the passwords for financial websites that would like to gain the access to banking websites

OFFLINE ATTACKS

- Offline attacks require physical access to the computer and copying the password file from the system on to removable media. Different types of offline password attacks are
  - a) Dictionary attack
  - b) Hybrid attack
  - c) Brute force attack
- Non-electronic attacks:
- Different types of Non-electronic attacks are
  - a) Social engineering
  - b) Shoulder surfing
  - c) Dumpster diving

CONT . . .

- **Social engineering :-**Is a method of using psychology to gain access to the computer systems and tricking the victims into giving out sensitive and personal information such as passwords and other credentials. The most common social engineering techniques are Phishing, Vishing, etc.
- **Shoulder surfing :-** It is a technique of gathering information such as username and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.
- **Dumpster diving:-** In the IT world, dumpster diving refers to using various methods to get information about a technology user. In general, dumpster diving involves looking in the trash for information written on pieces of paper or computer printouts. This is often done to uncover useful information that may help an individual get access to a particular network.

WHAT IS A KEYLOGGER?

- Keystroke logging, often called keylogging, is the practice of noting or logging the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.

CONT . . .

- A keylogger is a program that runs in the background or hardware, recording all the keystrokes.
- Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker.
- Attacker checks files carefully in the hopes of either finding passwords, or possibly other useful information.
- Keyloggers, as a surveillance tool, are often used by employers to ensure employees use computers for business purposes only.
- This method is highly useful for law enforcement and for the practice of spying. Typically by governments to obtain political and military information.
- Besides being used for legitimate (authenticated) purposes, keyloggers can be used to collect sensitive information.

TYPES OF KEYLOGGERS

- There are two types of keyloggers.
- 1. Software Keyloggers
- 2. Hardware keyloggers
- Software Keyloggers :- Software 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.
- Cybercriminals always install such tools on the insecure computer systems available in public places and can obtain the required information about the victim very easily.
- Software keyloggers track system, collect keystroke data within the target operating system, store them on disk or in remote location, and send them to the attacker who installed the keyloggers.

CONT...

- Anti-malware, personal firewall, and Host-based Intrusion prevention solution (HIPS) detect and remove application keyloggers.
- A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystroke
- Some of the examples of software keyloggers are
  - All in One Keylogger
  - Perfect Keylogger
  - KGB Spy
  - Elite Keylogger
  - Spy Buddy
  - CyberSpy
  - Powered Keylogger, etc.

HARDWARE KEYLOGGERS

- To install these keyloggers, physical access to the computer system is required.
- Hardware keyloggers are small hardware devices.
- These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- Cybercriminals install such devices on ATM machines to capture ATM Cards PINs.
- Each keypress on the keyboard of the ATM gets registered by these keyloggers.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

CONT …

- Some of the hardware keyloggers can be found from the following websites. 1. www.keyghost.com 2. www.keelog.com 3. www.keydevil.com 4. www.keykatcher.com
- **Antikeylogger:-** An anti-keylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool. In comparison to most anti-virus or anti-spyware software, the primary difference is that an anti-keylogger does not make a distinction between a legitimate keystroke-logging program and an illegitimate keystroke-logging program (such as malware).

ADVANTAGES

- Advantages of using anti-keylogger are as follows:
- Firewalls cannot detect the installations of keyloggers on the systems. Hence, anti-keyloggers can detect installation of keylogger.
- This software does not require regular updates of signatures bases to work effectively such as other anti-virus programs.
- Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
- It prevents ID theft.
- It secures E-Mail and instant messaging/chatting

ATTACK ON WIRELESS NETWORKS

- Wireless technologies have become increasingly popular in day-today business and personal lives.
- Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet.
- Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wirelessenabled devices such as laptops and PDAs
- Wireless networks are generally composed of two basic elements
- Access points (APs)
- Other wireless-enabled devices, such as laptops, radio transmitters and receivers to communicate or "connect" with each other
- Wireless access to networks has become very common in India both for organizations and for individuals.

HOW TO SECURE THE WIRELESS NETWORKS

- Nowadays, security features of Wi-Fi networking products are not that time-consuming. However, they are still ignored by home users.
- The following summarized steps will help to improve and strengthen the security of wireless network.
  1. Change the default settings of all the equipments/components of wireless network (e.g., IP address/user IDs/administrator passwords, etc).
  2. Enable WPA/WEP encryption.
  3. Change the default SSID.
  4. Enable MAC address filtering.
  5. Disable remote login.
  6. Disable SSID broadcast.
  7. Disable the features that are not used in the AP (e.g., printing/music support).

CONT...

1. Avoid providing the network a name which can be easily identified (e.g., My_Home_Wifi).
2. Connect only to secured wireless network (i.e., do not auto connect to open Wi-Fi hotspots).
3. Upgrade router's firmware periodically.
4. Assign static IP addresses to devices.
5. Enable firewalls on each computer and the router.
6. Position the router or AP safely.
7. Turn off the network during extended periods when not in use.
8. Periodic and regular monitor wireless network security.

SOME OF THE TOOLS USED TO PROTECT WIRELESS NETWORK ARE

- Zamzom Wireless Network Tool
- AirDefense Guard
- Wireless Intrusion Detection System (WIDZ)
- BSD-Airtools
- Google Secure Access

THANK YOU