System Hacking

LECTURE 7

System-Hacking Process

Password Cracking:

- ❑ Collected a wealth of information, including usernames>> give you something on which to focus your attack more closely.
- ❑ You use password cracking to obtain the credentials of a given account with the intention of using the account to gain authorized access to the system under the guise of a legitimate user.

How Passwords are designed?

A password is designed to be something an individual can remember easily but at the same time not something that can be easily guessed or broken.

This is where the problem lies ☺ ☺

Human beings tend to choose passwords that are *easy to remember, which can make them easy to guess*. Although choosing passwords that are easier to remember is not a bad thing, it can be a liability if individuals choose passwords that are too simple to guess.

Examples of easily cracked passwords

- Passwords that use only numbers
- Passwords that use only letters
- Passwords that are all upper- or lowercase
- Passwords that use proper names
- Passwords that use dictionary words
- Short passwords (fewer than eight characters)

Passwords are quickly losing their effectiveness

Passwords are quickly losing their effectiveness as a security measure on their own. In fact, in increasing numbers companies are moving to or are evaluating systems that use multifactor authentication.

passds are supplemented with smart cards, biometrics, RSA tokens, or other mechanisms, making the authentication process stronger.

Password-Cracking Techniques

Dictionary Attacks An attack of this type takes the form of a password-cracking application that has a dictionary file loaded into it. The dictionary file is a text file that contains a list of known words up to and including the entire dictionary. The application uses this list to test different words to recover the password. Systems that use passphrases typically are not vulnerable to this type of attack.

Brute-Force Attacks In this type of attack, every possible combination of characters is attempted until the correct one is uncovered. According to RSA Labs, “Exhaustive key search, or brute-force search, is the basic technique for trying every possible key in turn until the correct key is identified.”

Password-Cracking Techniques Cont.

Hybrid Attack This form of password attack builds on the dictionary attack but with additional steps as part of the process. In most cases, this means passwords that are tried during a dictionary attack are modified with the addition and substitution of special characters and numbers, such as *P@ssw0rd* instead of *Password.*

Syllable Attack This type of attack is a combination of a brute-force attack and a dictionary attack. It is useful when the password a user has chosen is not a standard word or phrase.

Rule-Based Attack This could be considered an advanced attack. It assumes that the user has created a password using information the attacker has some knowledge of ahead of time, such as phrases and digits the user may have a tendency to use.

Passive Online Attacks in this category are carried out simply by sitting back and listening—in this case, via technology, in the form of sniffing tools such as Wireshark, man-in-the-middle attacks, or replay attacks.

Password-Cracking Techniques Cont.

Active Online Attacks The attacks in this category are more aggressive than passive attacks because the process requires deeper engagement with the targets. Attackers using this approach are targeting a victim with the intention of breaking a password. In cases of weak or poor passwords, active attacks are very effective. Forms of this attack include password guessing, Trojan/spyware/key loggers, hash injection, and phishing.

Offline Attacks This type of attack is designed to prey on the weaknesses not of passwords but of the way they are stored. Because passwords must be stored in some format, an attacker seeks to obtain them where they are stored by exploiting poor security or weaknesses inherent in a system. If these credentials happen to be stored in a plaintext or unencrypted format, the attacker will go after this file and gain the credentials. Forms of this attack include precomputed hashes, distributed network attacks, and rainbow attacks.

Passive online attacks

Packet Sniffing: A sniffer, or packet analyzer, as it also called, is a mechanism (typically software) designed to capture packets as they flow across the network.

Basically, anything that uses clear text to transmit credentials is going to be vulnerable. If a password is sent in an encrypted format, it doesn’t mean you won’t be able to intercept the password, just that you won’t be able to read it.

Replay Attack

After the relevant information is captured and extracted, the packets can be placed back on the network. The intention is to inject the captured information—such as a password—back onto the network and direct it toward a resource such as a server, with the goal of gaining access.

Once the packets are replayed, the valid credentials provide access to a system, potentially giving an attacker the ability to change information or obtain confidential data

Active Online Attacks

Trojans, Spyware, and Keyloggers:

One form is keyboard sniffing or keylogging, which intercepts a password as the user enters it. This attack can be carried out when users are the victims of keylogging software or if they regularly log on to systems remotely without using protection.

Offline Attacks

Precomputed Hashes or Rainbow Tables:

Precomputed hashes are used in an attack type known as a rainbow table. Rainbow tables compute every possible combination of characters prior to capturing a password. Once all the passwords have been generated, the attacker can capture the password hash from the network and compare it with the hashes that have already been generated.

With all the hashes generated ahead of time, it becomes a simple matter to compare the captured hash to the ones generated, typically revealing the password in a few moments.

Other Options for Obtaining Passwords

Default Passwords

One of the biggest potential vulnerabilities is also one of the easiest to resolve: default passwords. Default passwords are set by the manufacturer when the device or system is built. They are documented and provided to the final consumer of the product and are intended to be changed.

anyone can look up your default password at any of the following sites:

http://cirt.net

http://default-password.info

www.defaultpassword.us

www.passwordsdatabase.com

https://w3dt.net

www.virus.org

http://open-sez.me

Cont.

Guessing: *old school*

1. Locate a valid user.

2. Determine a list of potential passwords.

3. Rank possible passwords from least to most likely.

4. Try passwords until access is gained or the options are exhausted.

Cont.

USB Password Theft:

This method entails embedding a password-stealing application on a USB drive and then physically plugging the drive into a target system.

Because many users store their passwords for applications and online sites on their local machine, the passwords may be easily extracted.