GOALS OF SYSTEM HACKING

- **Gaining Access**
- **Escalating privileges**
- **Executing applications**
- **Hiding files**
- **Clearing tracks**

GAINING ACCESS

The goal here is to collect enough information to gain access to the target.

Password Cracking:

There are few basic methods of password cracking:

Bruteforce: trying all possible combinations until the password is cracked.

Dictionary attack: This is a compiled list of meaningful words, compared against the password field till a match is found.

Rule based attack: If some details about the target are known, we can create rules based on the information we know.

Rainbow table: Instead of comparing the passwords directly, taking the hash value of the password, comparing them with a list of pre-computed hash values until a match is found.

Rainbow table method gives an advantage to the attacker since no account lockout is enabled for wrong hashes against the password. To prevent rainbow table attack, salting can be used. Salting is a process of adding random numbers to the password so the attacker will not be able to crack the hash without that salt added.

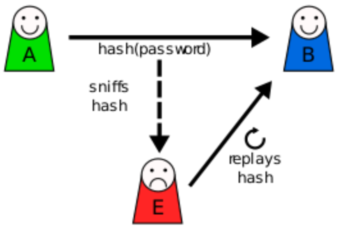
Types of Password Attacks

Passive online attacks

A passive attack is an attack on a system that does not result in a change to the system in any way.

The attack is to purely monitor or record data.

- Wire Sniffing
- Man in the middle
- Replay attack



Active online attack

An active online attack is the easiest way to gain unauthorized administrator-level access to the system

- Password guessing
- Trojan/spyware/keyloggers

- Hash injection
- Phishing

Offline attacks

Offline attacks occur when the intruder checks the validity of the passwords. Offline attacks are often time to consume.

- Pre-computed hashes
- Distributed Network
- Rainbow

Non-electronic attacks

Non-electronic attacks are also known as non-technical attacks. This kind of attack doesn't require any technical knowledge about the methods of intruding into another system.

- Social engineering
- Shoulder surfing
- Dumpster Diving

How to defend against password cracking:

- Don't share your password with anyone
- Do not use the same passwords during password change
- Enable security auditing to help monitor and track password attack
- Do not use clear text protocols and protocols with weak encryption
- Set the password change policy to 30 days
- Monitor the server's logs for brute force attacks on the user's accounts
- Avoid storing passwords in an unsecured location
- Never use passwords such as date of birth, spouse, or child's or pet's name
- Enable SYSKEY with the strong password to encrypt and protect the SAM database
- Lockout an account subjected to too many incorrect password guesses.

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 privilege.

Escalation of Privileges:

There are **two types** of Privilege Escalation:

Horizontal Privilege Escalation occurs when a malicious user attempts to access resources and functions that belong to peer users, who have similar access permissions.

Vertical Privilege Escalation occurs when a malicious user attempts to access resources and functions that belong to a user with higher privileges, such as application or site administrators

EXECUTING APPLICATIONS

Intruder executes malicious applications after gaining administrative privileges so they can run malicious programs remotely, to capture all sensitive data, crack passwords, capture screenshots or to install a backdoor.

Tool: RemoteExec, PDQ Deploy, DameWare NT Utilities

Keylogger

keystroke loggers are programs or hardware devices that monitor each keystroke a user types on a keyboard, logs onto a file, or transmits them to a remote location.

keyloggers are placed between the keyboard hardware and the OS

A key logger can

- Record each keystroke
- capture screenshots at regular intervals of time showing user activity such as when he or she types a character or click a mouse button
- Track the activities of users by logging window titles, names of launched applications and other information
- monitor online activity of users by recording addresses of the websites that they are have visited and with the keywords entered by them
- record all the login names, bank and credit card numbers and passwords including hidden passwords or data that are in asterisk or blank spaces
- record online chat conversion

Types of Keylogger

- Hardware Keylogger
- Software Keylogger

Spyware

Spyware is stealthy computer monitoring software that allows you to secretly record all activities of a computer user.

HIDING FILES

Rootkits

Rootkits are programs that hackers use in order to evade detection while trying to gain unauthorized access to a computer. Rootkits when installing on a computer, are invisible to the user and also take steps to avoid being detected by security software.

A rootkit is a set of binaries, scripts and configuration files that allows someone to covertly maintain access to a computer so that he can issue commands and scavenge data without alerting the system's owner.

Depending on where they are installed there are various types of rootkits:

Kernel Level Rootkits

Hardware/Firmware Rootkits

Hypervisor (Virtualized) Level Rootkits

Boot loader Level (Bootkit) Rootkits

NTFS DATA Stream

Alternative Data Stream support was added to NTFS (Windows NT, Windows 2000 and Windows XP) to help support Macintosh Hierarchical File System (HFS) which uses resource forks to store icons and other information for a file. Using Alternative Data Streams a user can easily hide files that can go undetected unless close inspection.

Steganography

The art of hiding a data inside another data/medium is called steganography.

For eg: hiding data within an image file

The secret message is called overt file and the covering file is called covert file.

Types of Steganography

- Image Steganography
- Document Steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- White Space Steganography