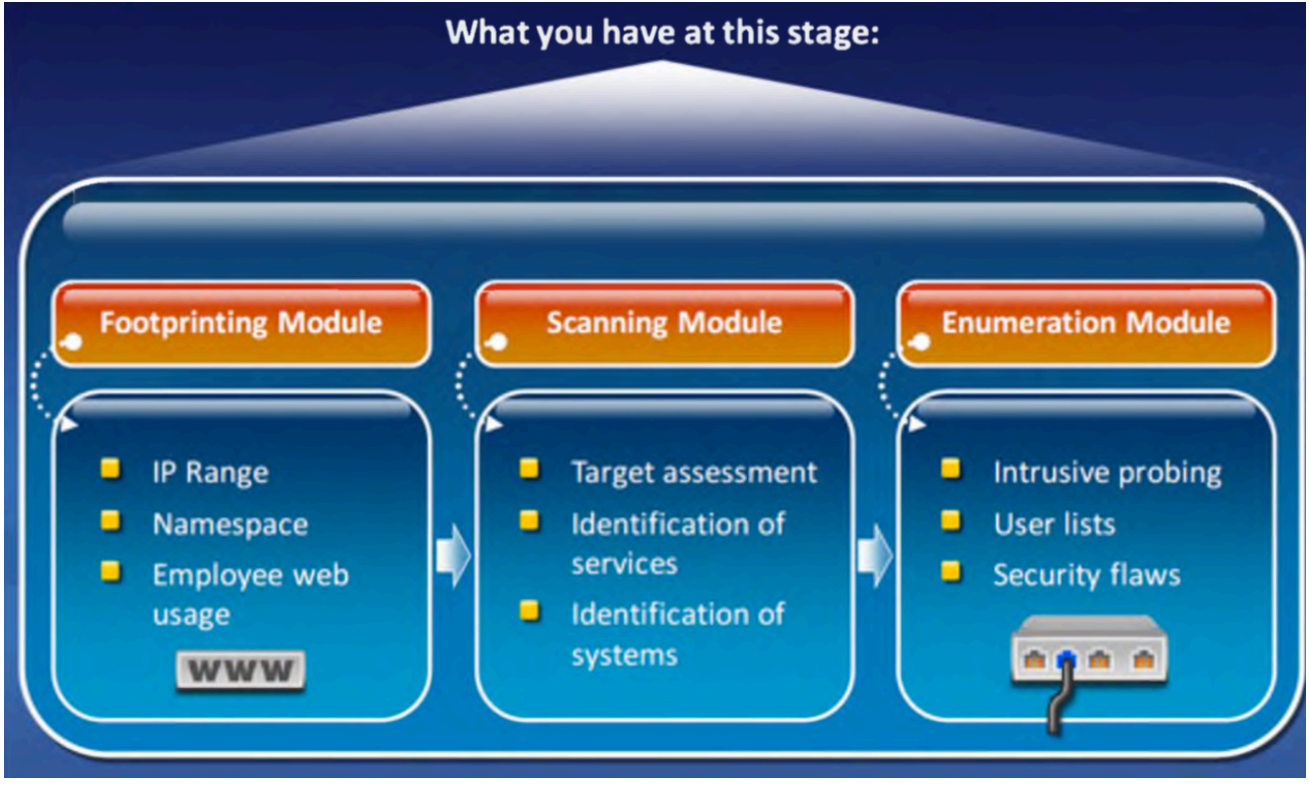
Computer System Hacking

Prepared by:
Dr. Ahmed Redha
PSU

Information at Hand Before System Hacking Stage



Gaining Access

❖ Microsoft Authentication

- Windows uses the Security Accounts Manager (SAM) database or Active Directory Database to manage user accounts and passwords in hashed format (a one-way hash).
- The system does not store the passwords in plaintext format but in a hashed format, to protect them from attacks.
- The system implements the SAM database as a registry file, and the Windows kernel obtains and keeps an exclusive filesystem lock on the SAM file. As this file consists of a filesystem lock, this provides some measure of security for the storage of passwords.

Uses hashes

Cannot copy SAM while system is running

- It is not possible to copy the SAM file to another location in the case of online attacks. Because the system locks the SAM file with an exclusive filesystem lock, a user cannot copy or move it while Windows is running.
- The lock does not release until the system throws a blue screen exception, or the OS has shut down. However, to make the password hashes available for offline brute-force attacks, attackers can dump the on-disk contents of the SAM file using various techniques.

❖ NTLM Authentication

weak

- NT LAN Manager (NTLM) is a default authentication scheme that performs authentication using a challenge/response strategy. Because it does not rely on any official protocol specification, there is no guarantee that it works effectively in every situation.
- Furthermore, it has been used in some Windows installations, where it successfully worked. NTLM authentication consists of two protocols: NTLM authentication protocol and LAN Manager (LM) authentication protocol.
- These protocols use different hash methodologies to store users' passwords in the SAM database.

❖Kerberos Authentication

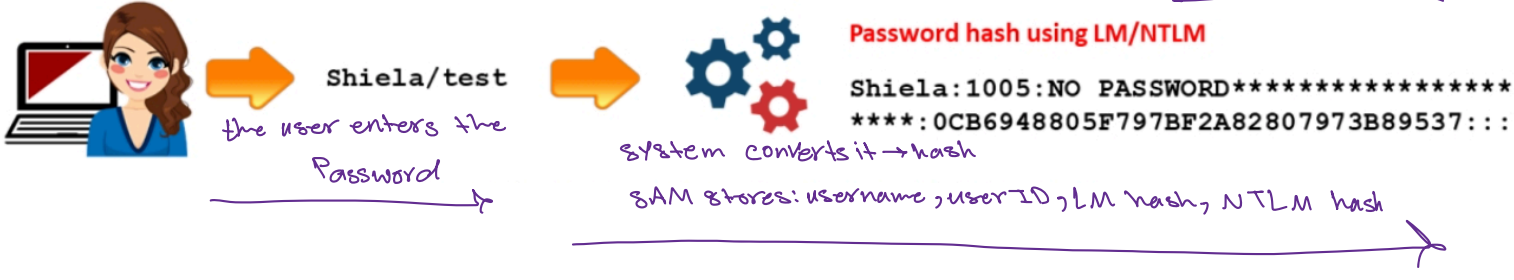
- Kerberos is a network authentication protocol that provides strong authentication for client/server applications through secret-key cryptography. This protocol provides mutual authentication, in that both the server and the user verify each other's identity.
- Messages sent through Kerberos protocol are protected against replay attacks and eavesdropping.
- Microsoft has upgraded its default authentication protocol to Kerberos, which provides a stronger authentication for client/server applications than NTLM

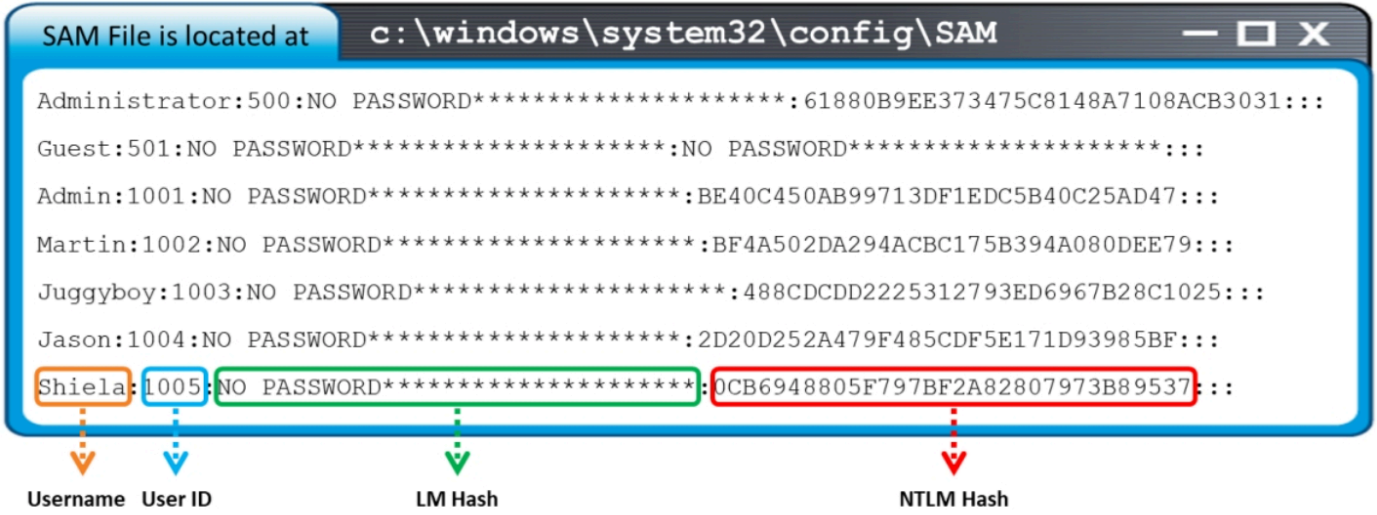
How Hash Passwords Are Stored in Windows SAM?

Windows OSs use a Security Account Manager (SAM) database file to store user passwords. The SAM file is stored at %SystemRoot%/system32/config/SAM in Windows systems, and Windows mounts it in the registry under the HKLM/SAM registry hive. It stores LM or NTLM hashed passwords.

Windows does not store Passwords directly.

it stores hashed Passwords inside the SAM file




SAM File is located at
c:\windows\system32\config\SAM
Administrator:500:NO PASSWORD**********:61880B9EE373475C8148A7108ACB3031:::
Guest:501:NO PASSWORD**********:NO PASSWORD**********:::
Admin:1001:NO PASSWORD**********:BE40C450AB99713DF1EDC5B40C25AD47:::
Martin:1002:NO PASSWORD**********:BF4A502DA294ACBC175B394A080DEE79:::
Juggyboy:1003:NO PASSWORD**********:488CDCDD2225312793ED6967B28C1025:::
Jason:1004:NO PASSWORD**********:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1005:NO PASSWORD**********:0CB6948805F797BF2A82807973B89537:::
Username
User ID
LM Hash
NTLM Hash

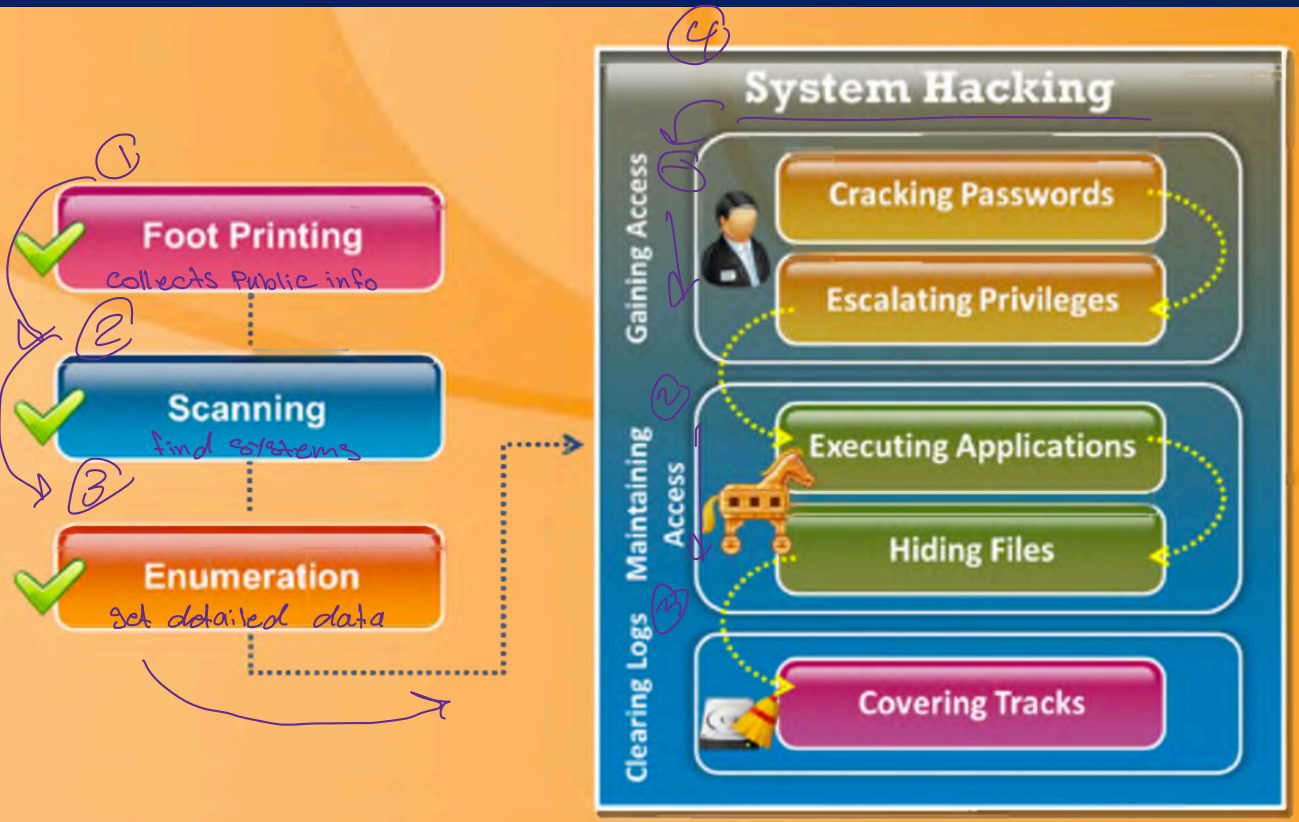
SAM file

System Hacking: Goals

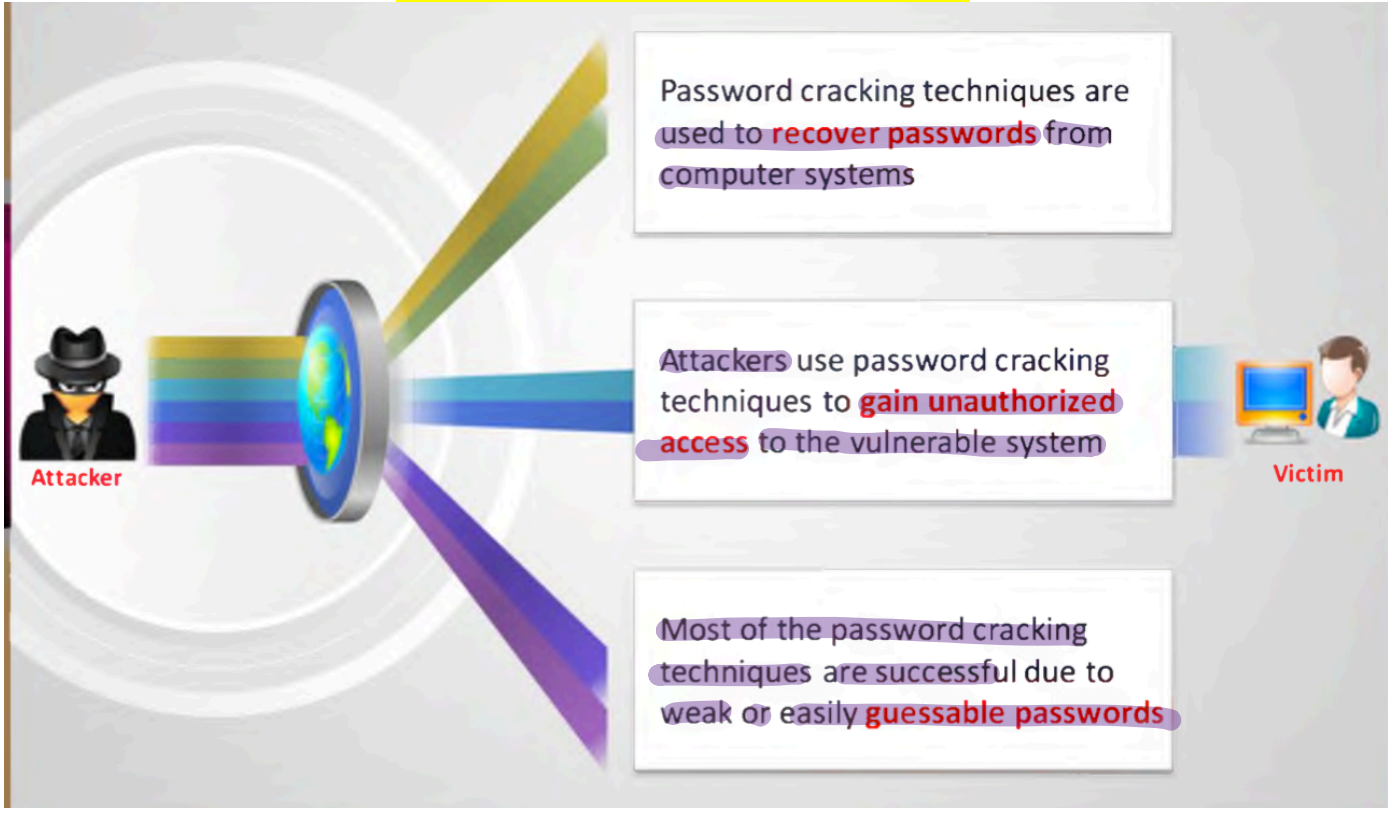
Hacking-Stage	Goal	Technique/Exploit Used
1 Gaining Access	To bypass access controls to gain access to the system	Password cracking, social engineering
2 Escalating Privileges	To acquire the rights of another user or an admin	Exploiting known system vulnerabilities
3 Executing Applications	To create and maintain remote access to the system	Trojans, spywares, backdoors, keyloggers
4 Hiding Files	To hide attackers malicious activities and data theft	Rootkits, steganography
5 Covering Tracks	To hide the evidence of compromise	Clearing logs

Gaining Access : CEH Hacking Methodology (CHM)

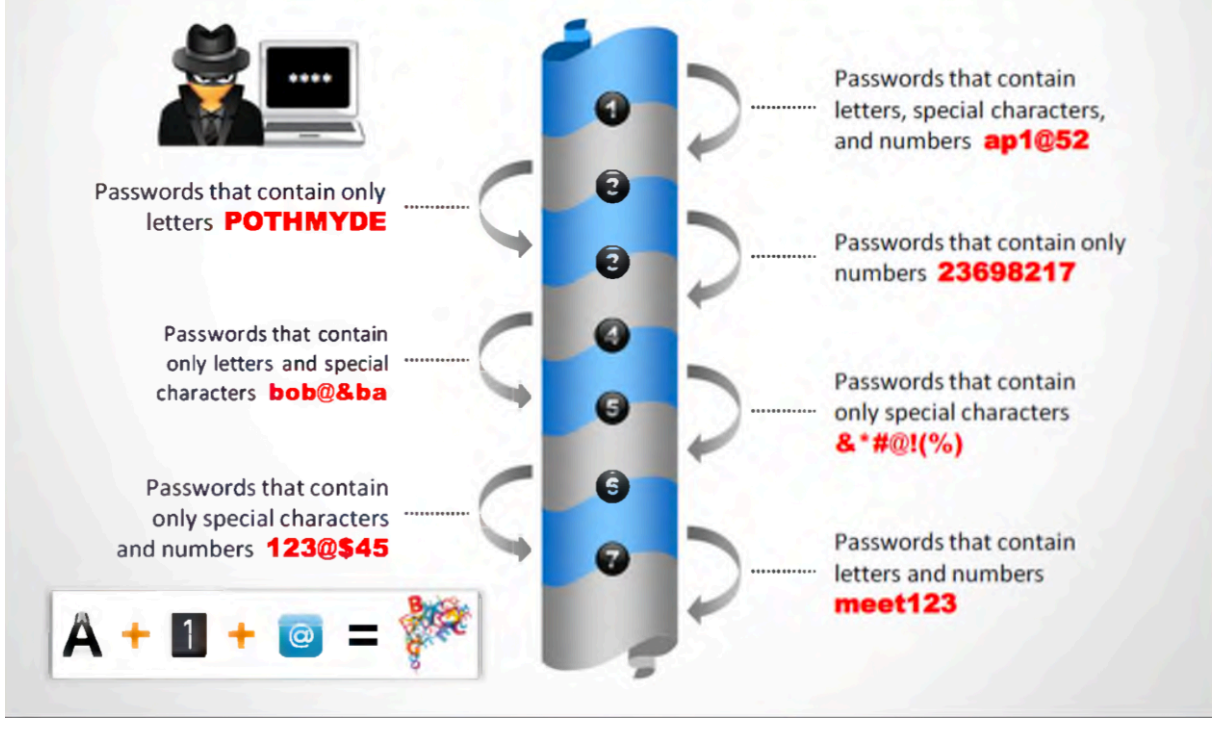
- Before hacking a system, an attacker uses footprinting, scanning, and enumeration techniques to detect the target area of the attack and the vulnerabilities that prove to be doorways for the attacker.
- Once the attacker gains all the necessary information, he or she starts hacking.
- Like the attacker, an ethical hacker also follows the same steps to test a system or network. To ensure the effectiveness of the test, the ethical hacker follows the hacking methodology. The following diagram depicts the hacking methodology followed by ethical hackers:


Foot Printing
collects public info
Scanning
find systems
Enumeration
get detailed data
System Hacking
Gaining Access
Cracking Passwords
Escalating Privileges
Maintaining Access
Executing Applications
Hiding Files
Clearing Logs
Covering Tracks

Password Cracking



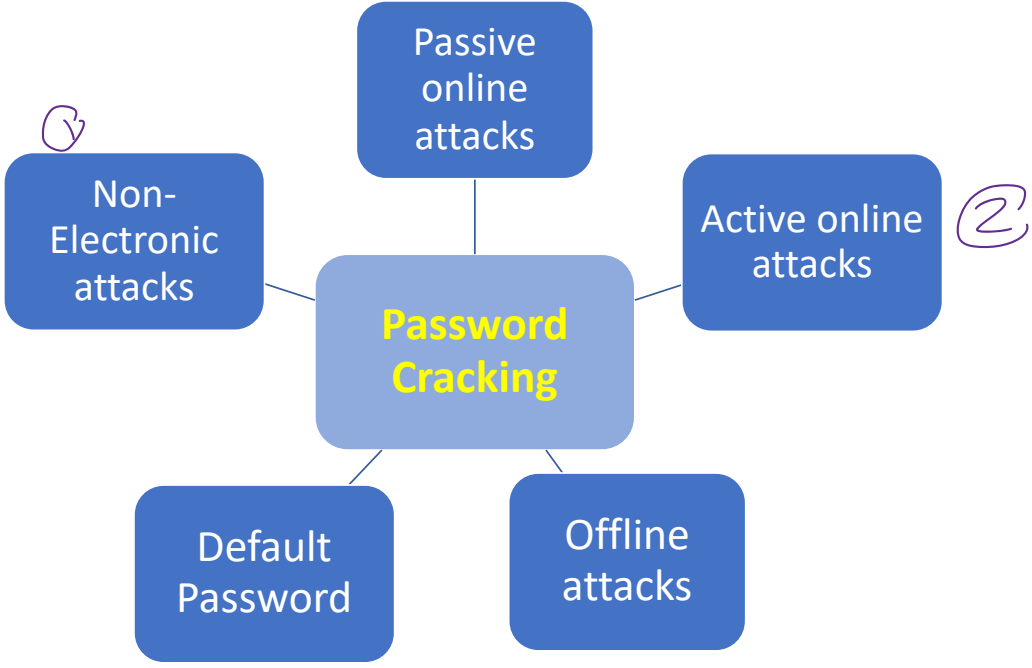
Password Complexity



Password Cracking Techniques

Password cracking is the technique used for discovering passwords. It is the classic way to gain privileges to a computer system or network. The common approach for cracking a password is to continually try guesses for the password with various combinations until you get the correct one. There are five techniques for password cracking:

Types of Password Cracking



1- Non-Electronic attack

Non-Electronic attack known as non-technical attacks. This kind of attack doesn't require any technical knowledge about the methods of intruding into another's system. Therefore, it is called a non-electronic attack. There are three types of non-electronic attacks. They are:

- Shoulder surfing S: watching someone type their password
- Social engineering
- Dumpster diving

2- Active Online Attacks

Attacker performs password cracking by directly communicating with the victim machine.

2.1 Dictionary and Brute Forcing Attack

trying many Passwords

2.2 Trojan/Spyware/Keyloggers

recording keystrokes

2.3 Hash Injection and Phishing

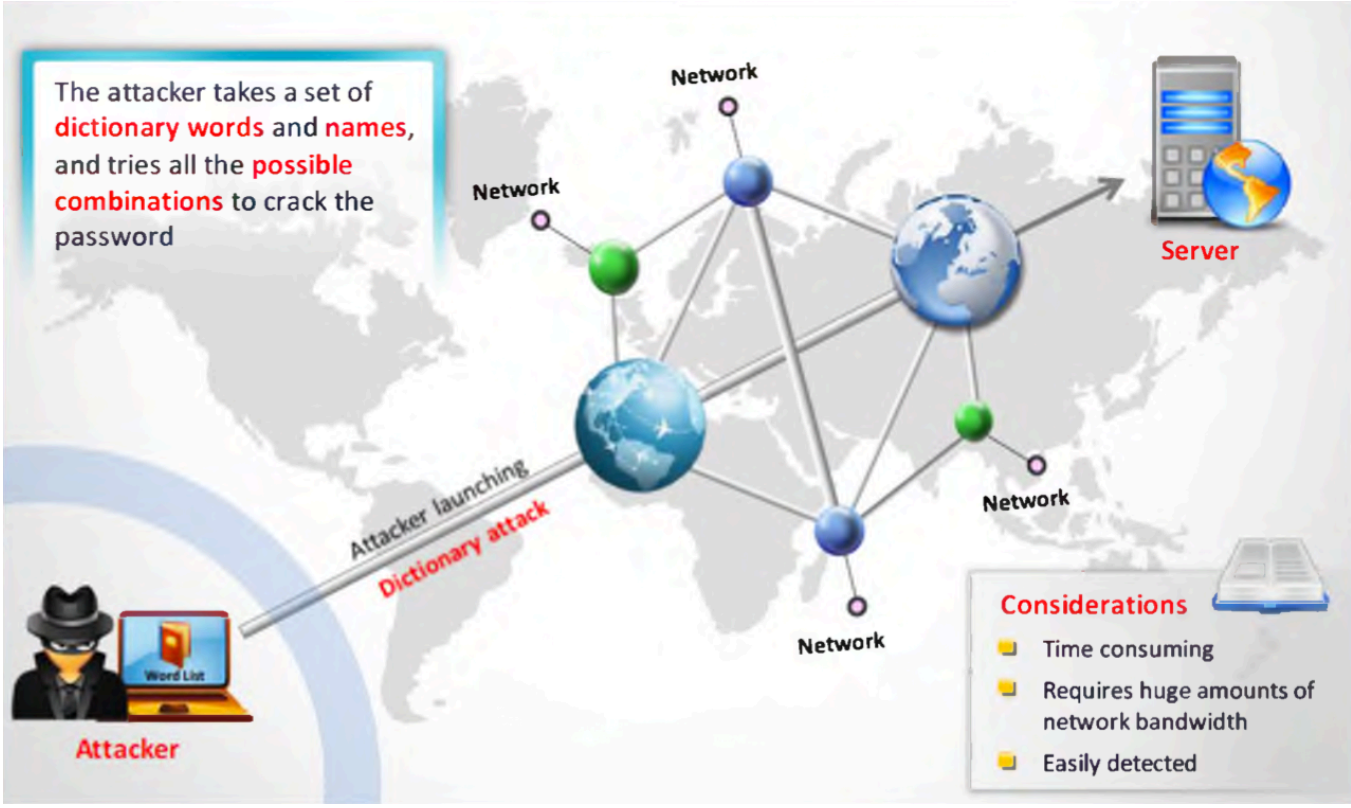
Fake login Page

2.1 Active Online Attack: Dictionary and Brute Forcing Attack

- In this type of attack, a dictionary file is loaded into a cracking application that runs against user accounts. This dictionary is a text file that contains several dictionary words commonly used as passwords.
- The program uses every word present in the dictionary to find the password. In addition to a standard dictionary, an attackers' dictionaries contain entries with numbers and symbols added to words (e.g., "3December!962").
- Simple keyboard finger rolls ("qwer0987"), which many believe to produce random and secure passwords, are thus included in such a dictionary. Dictionary attacks are more useful than brute-force attacks, however, the former cannot be performed in systems using passphrases.

This attack is applicable in two situations:

1. In cryptanalysis, to discover the decryption key for obtaining the plaintext from a ciphertext
2. In computer security, to bypass authentication and access the control mechanism of the computer by guessing passwords


The attacker takes a set of dictionary words and names, and tries all the possible combinations to crack the password
Network
Network
Server
Network
Network
Attacker launching
Dictionary attack
Word List
Attacker
Considerations
Time consuming
Requires huge amounts of network bandwidth
Easily detected

Methods to improve the success of a dictionary attack:

- Use of several different dictionaries, such as technical and foreign dictionaries, which increases the number of possibilities
- Use of string manipulation along with the dictionary (e.g., if the dictionary contains the word “system,” string manipulation creates anagrams like “metsys,” among others)

2.2 Active Online Attack: Trojan/Spyware/Keylogger

1

Spyware is a type of malware that allows attackers to secretly gather information about a person or organization

K.w

With the help of a Trojan, an attacker gets access to the stored passwords in the attacked computer and is able to read personal documents, delete files, and display pictures

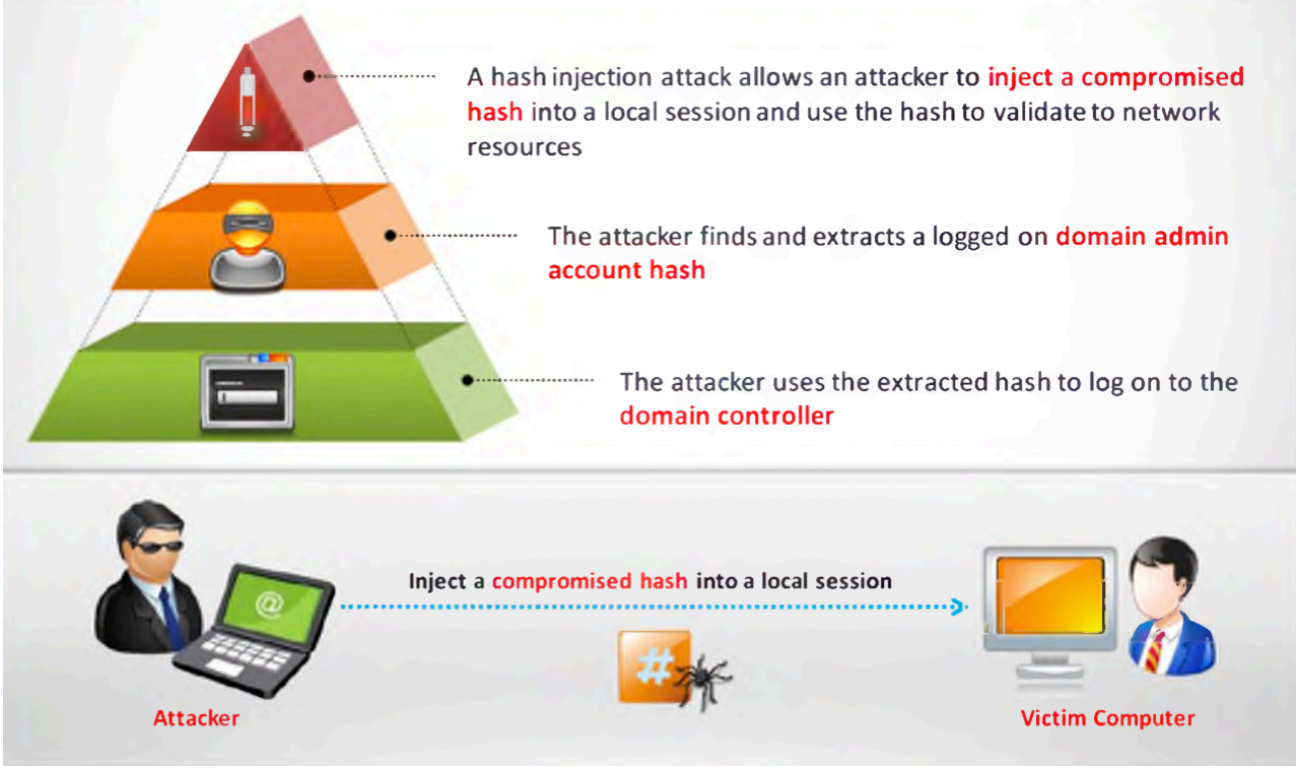
↳ From the help of trojan horse

2

3

A Keylogger is a program that runs in the background and allows remote attackers to record every keystroke

2.3 Active Online Attack: Hash Injection Attack

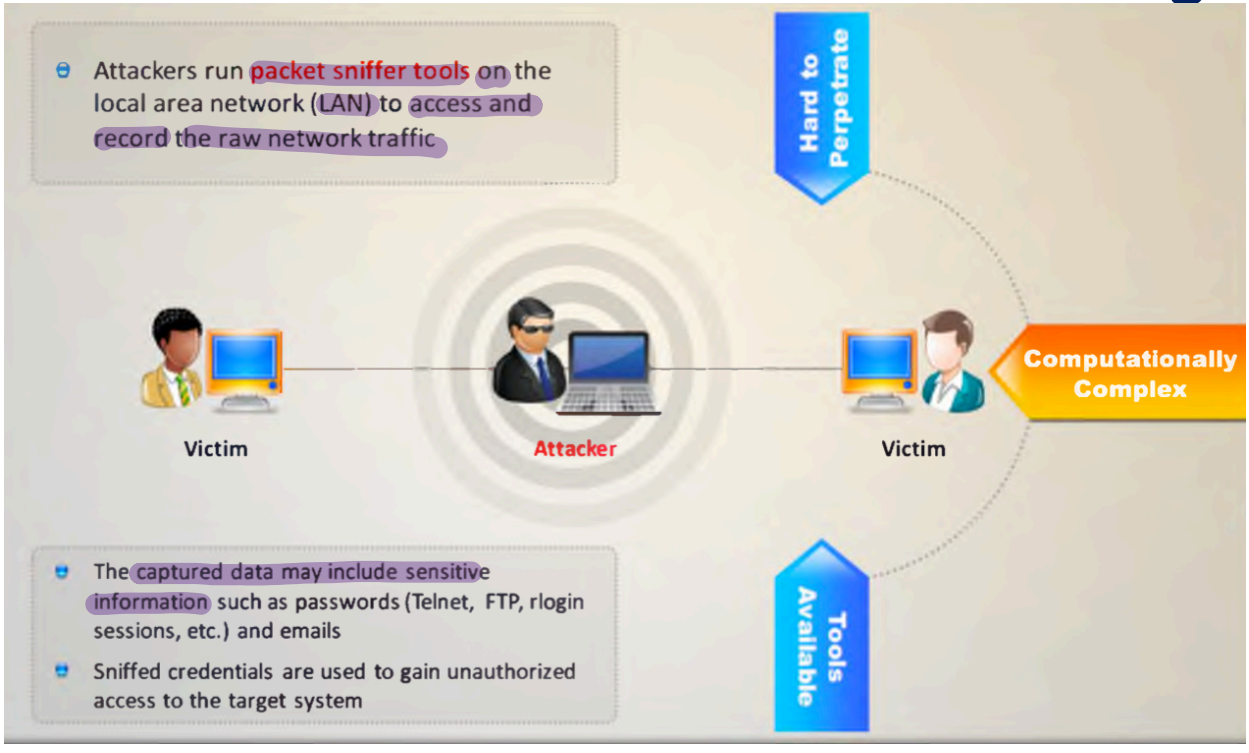


3- Passive Online Attacks

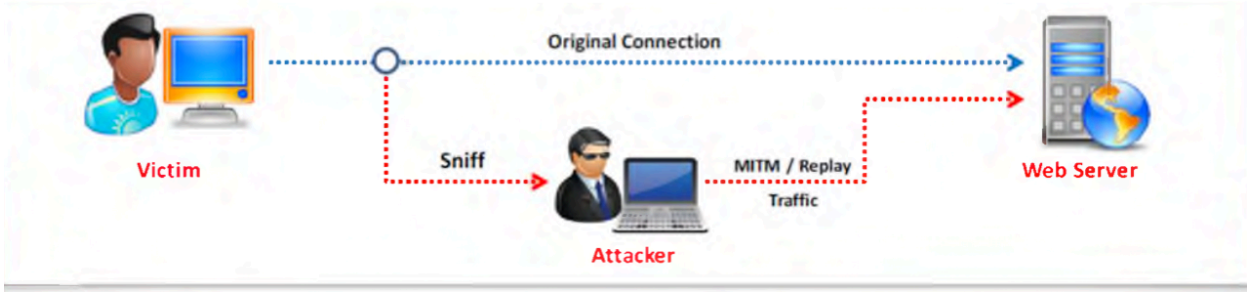
Attacker performs password cracking without communicating with the authorizing party.

- Wire Sniffing
- Man-in-the-Middle
- Replay

3.1 Passive Online Attack: Wire Sniffing



3.2 Passive Online Attack: Man-in-the -Middle and Replay Attack



Gain access to the communication channels

In a MITM attack, the attacker acquires access to the communication channels between victim and server to extract the information

Use sniffer

In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access

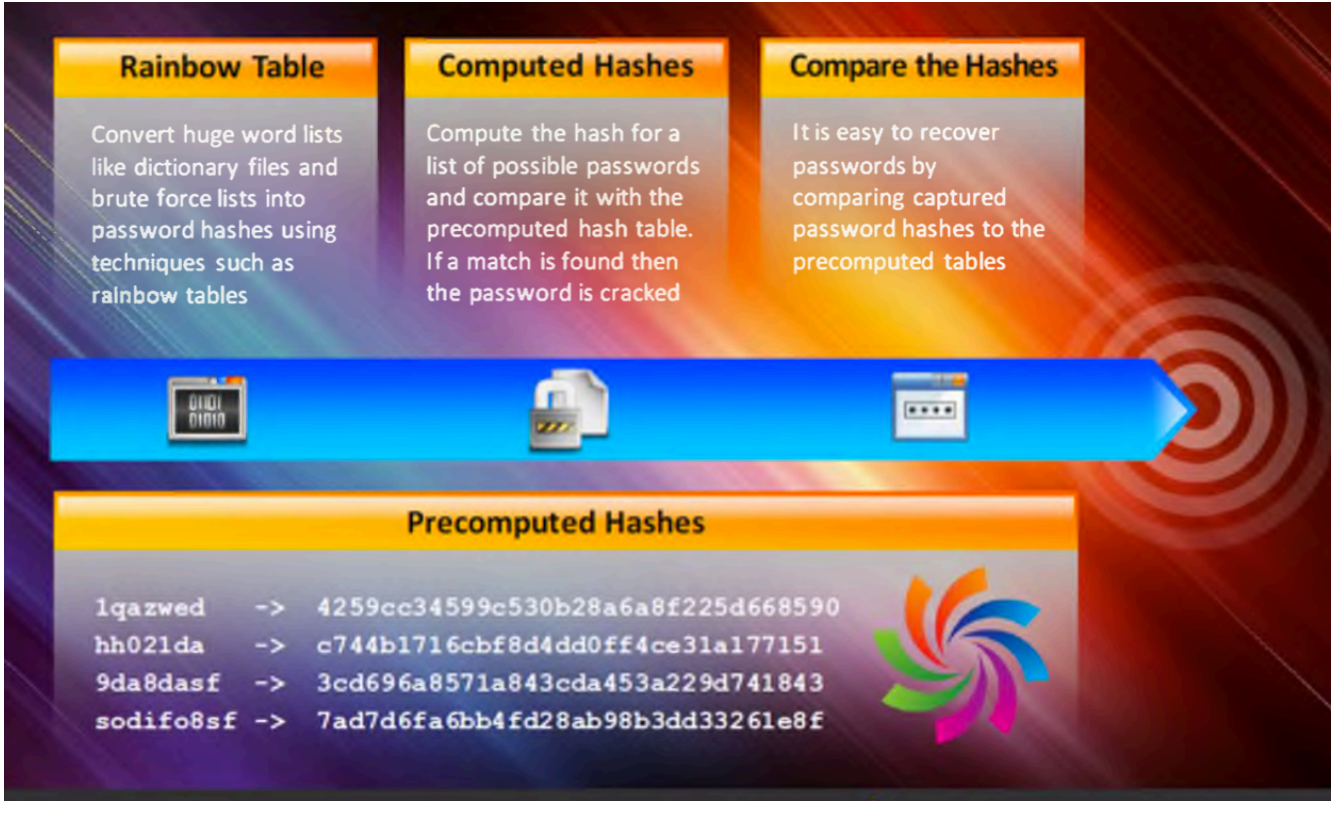
Considerations

- Relatively **hard to perpetrate**
- Must be **trusted** by one or both sides
- Can sometimes be broken by **invalidating traffic**

4- Offline Attack: Rainbow Attacks

- Offline attacks occur when an attacker checks the validity of passwords. The attacker observes how the password is stored. If the usernames and passwords are stored in a readable file, it is easy for the attacker to gain access to the system. Hence, it is important to protect the list of passwords and keep it in an unreadable form, preferably encrypted.
- Offline attacks are often time-consuming but have a high success rate as the password hashes can be reversed owing to their small keyspace and short length. Notably, different password-cracking techniques are available on the Internet.

4- Offline Attack: Rainbow Attacks



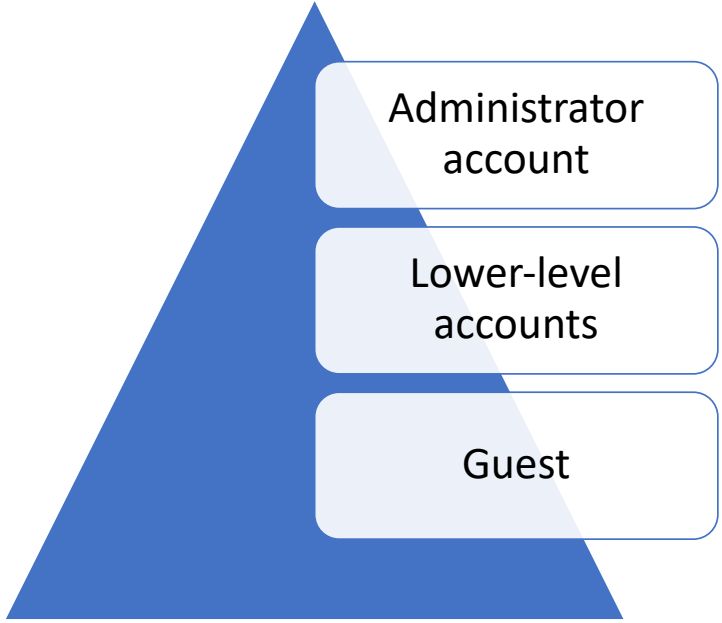
5- Default Password

Default passwords are those supplied by manufacturers with new equipment (e.g., switches, hubs, routers). Usually, default passwords provided by the manufacturers of password-protected devices allow the user to access the device during the initial setup and then change the password. However, often an administrator will either forget to set the new password or ignore the password-change recommendation and continue using the original password. Attackers can exploit this lapse and find the default password for the target device from manufacturer websites or using online tools that show default passwords to access the target device successfully. Attackers use default passwords in the list of words or dictionary that they use to perform password-guessing attacks.

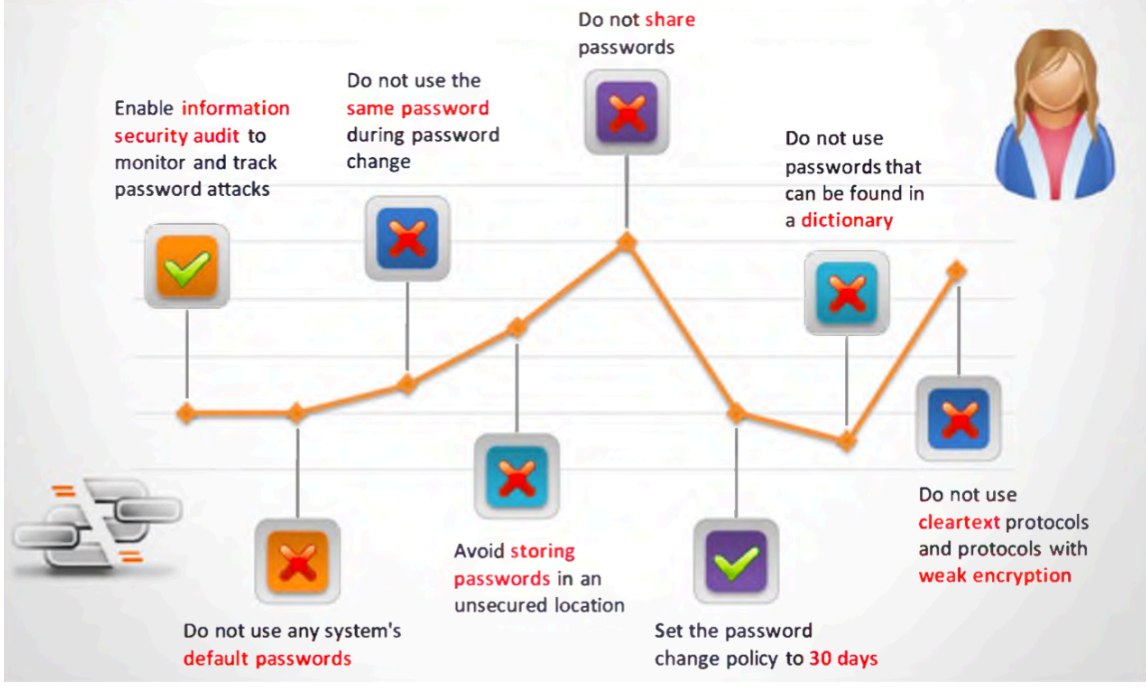
The following are some of the online tools to search default passwords:

- https://open-sez.me
- https://www.fortypoundhead.com
- https://cirt.net
- http://www.defaultpassword.us
- https://www.routerpasswords.com
- https://default-password.info
- https://192-168-1-1ip.mobi

Using Password Cracking: Targets



How to Defend against Password Cracking



Privilege Escalation

- Escalating privileges is the second stage of system hacking. Attackers use passwords obtained in the first step to gain access to the target system and then try to attain higher-level privileges in the system.
- An attacker can gain access to the network using a non-admin user account, and the next step would be to gain administrative privileges.
- Attacker performs privilege escalation attack which takes advantages of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.
- These privileges allow attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

Types of Privilege Escalation:

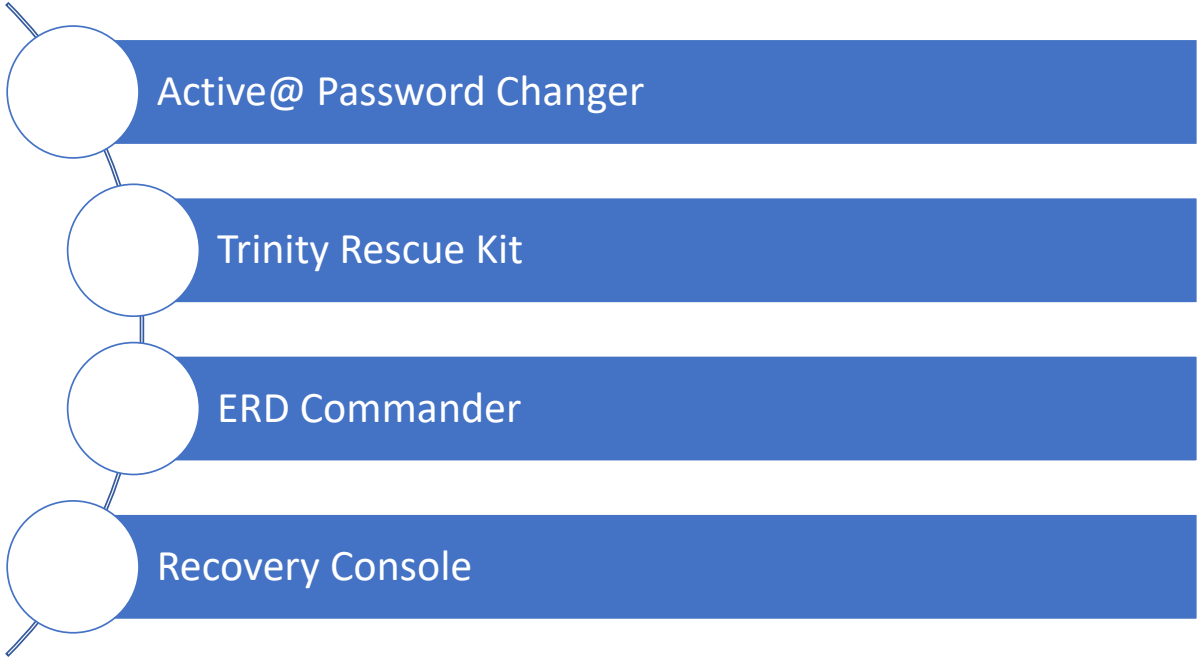
①Vertical Privilege Escalation

- Refers to gaining higher privileges than the existing

② Horizontal Privilege Escalation:

- The unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions. For instance, online banking user A can easily access user B's bank account.

Privilege Escalation Tools



Maintaining Access

- After gaining access and escalating privileges on the target system, now attackers try to maintain their access for further exploitation of the target system or make the compromised system a launchpad from which to attack other systems in the network.
- Attackers remotely execute malicious applications such as keyloggers, spyware, and other malicious programs to maintain their access to the target system and steal critical information such as usernames and passwords.
- Attackers hide their malicious programs or files using rootkits, steganography, NTFS data streams, etc. to maintain their access to the target system.

Executing Applications

- Once attackers gain higher privileges in the target system by trying various privilege escalation attempts, they may attempt to execute a malicious application by exploiting a vulnerability to execute arbitrary code. By executing malicious applications, the attacker can steal personal information, gain unauthorized access to system resources, crack passwords, capture screenshots, install a backdoor for maintaining easy access, etc.

- Attackers execute malicious applications at this stage in a process called “owning” the system. Once they acquire administrative privileges, they will execute applications. Attackers may even try to do so remotely on the victim’s machine to gather the same information as above.

The malicious programs attackers execute on target systems can be:

- **Backdoors**: Program designed to deny or disrupt the operation, gather information that leads to exploitation or loss of privacy, or gain unauthorized access to system resources.
- **Crackers**: Components of software or programs designed for cracking a code or passwords.
- **Keyloggers**: These can be hardware or software. In either case, the objective is to record each keystroke made on the computer keyboard.
- **Spyware**: Spy software may capture screenshots and send them to a specified location defined by the hacker. For this purpose, attackers have to maintain access to victims' computers. After deriving all the requisite information from the victim's computer, the attacker installs several backdoors to maintain easy access to it in the future.

PS/2 Keylogger

USB Keylogger

Wi-Fi Keylogger

Keylogger embedded inside the keyboard

Bluetooth Keylogger

Hardware Keylogger

Different types of Hardware Keyloggers

Covering Tracks

- Covering tracks is one of the main stages during system hacking. In this stage, the attacker tries to hide and avoid being detected or “traced out” by covering all “tracks,” or logs, generated while accessing the target network or computer.
- Erasing evidence is a must for any attacker who would like to remain obscure. It is a method used to evade a traceback. It starts with erasing the contaminated logs and possible error messages generated in the attack process.
- The attacker makes changes to the system configuration such that it does not log the future activities. By manipulating and tweaking event logs, the attacker tricks the system administrator into believing that there is no malicious activity in the system and that no intrusion or compromise has taken place.

Some techniques used for Covering Tracks:

The main activities that an attacker performs toward removing his/her traces on a computer are as follows:

- **Disabling auditing**
  - If auditing is disabled, attacker can deprive system owner of ability to detect activities that have been carried out.
- **Data hiding**
  - Hiding files placed on the system
  - Can use file attributes and Alternate Data Streams to hide files
- **Clearing Logs**
  - An attacker clears/deletes the system log entries corresponding to his/her activities.

Defending against Covering Tracks

The various countermeasures to overcome covered tracks are as follows:

▪ Activate the logging functionality on all critical systems. ▪ Conduct periodic audits on IT systems to ensure that the logging functionality is in accordance with the security policy.

▪ Ensure that new events do not overwrite old entries in the log files when the storage limit is exceeded.

▪ Configure the appropriate and minimal permissions necessary to read and write log files stored in critical systems

▪ Maintain a separate logging server in the DMZ so that all critical servers such as DNS server, mail server, and web server forward and store their logs on that server.

▪ Regularly update and patch OSes, applications, and firmware.

▪ Close all unused open ports and services.

▪ Encrypt the log files stored in the system so that they cannot be altered without an appropriate decryption key.

▪ Set log files to the “append only” mode to prevent the unauthorized deletion of log entries.

▪ Periodically back up the log files to unalterable media. ▪ Use restricted ACLs to secure the log files.