System Hacking

- Prepared by Dr. A. Haritha

Contents-Part-I

Simplest way to get a password

- Passwords key piece of information- to access a system,
- Users often select passwords that are easy to guess.
- Many reuse passwords or choose one that's simple—such as a pet's name—to help them remember it.
- Because of this human factor, most password guessing is successful if some information is known about the target.
- Information gathering and reconnaissance can help give away information that will help a hacker guess a user's password.
- Once a password is guessed or cracked, it can be the launching point for escalating privileges, executing applications, hiding files, and covering tracks.

If guessing a password fails,

- be cracked manually
- automated tools such as a
  - dictionary, brute-force method.

Types of Passwords

Characters that form a password:

- Only letters
- Only numbers
- Only Special Characters
- Letters and numbers
- Only letters and special characters
- Only numbers and special characters
- Letters, numbers, and special characters

Types of Passwords

- A strong password is less susceptible to attack by a hacker

The EC-Council, rules

- Must not contain any part of the user's account name
- Must have a minimum of eight characters

Must contain characters from at least three of the following categories:

- Nonalphanumeric symbols ($,:"%@!#)
- Numbers
- Uppercase letters
- Lowercase letters

Types of Password Attacks

- **Passive Online** Eavesdropping on network password exchanges.
  Passive online attacks include sniffing, man-in-the-middle, and replay attacks.

- **Active Online** Guessing the Administrator password.
  Active online attacks include automated password guessing.

- **Offline** Dictionary, hybrid, and brute-force attacks.

- **Nonelectronic** Shoulder surfing, keyboard sniffing, and social engineering.

Passive online Attack

Sniffing,:

- The password is captured during the authentication process and can then be compared against a dictionary file or word list.
- User account passwords are commonly *hashed or encrypted when sent on the network to* prevent unauthorized access and use.
- special tools in the hacker's toolkit can be used to break the algorithm.

Man-in-the-middle:

- hacker intercepts the authentication request and forwards it to the server.
- Inserting a sniffer between the client and the server, the hacker is able to sniff both connections and capture passwords in the process.

replay attacks:

- hacker intercepts the password en route to the authentication server and then captures and resends the authentication packets for later authentication.
- In this manner, the hacker doesn't have to break the password or learn the password through MITM but rather captures the password
- reuses the password-authentication packets later to authenticate as the client.

Active online Attack

- Password guessing.
- human factor involved in password creation works on weak passwords.
- Attempting to connect to an enumerated share (IPC$ or C$) and trying a username and password combination.
- Commonly used Administrator account and password combinations are words like Admin, Administrator, Sysadmin, or Password, or a null password.
- A hacker may first try to connect to a default Admin$, C$, or C:\Windows share.

To connect to the hidden C: drive share, for example, type the following command in the

- Run field (Start ➪ Run):
- *ip_address*\c$
- Automated programs can quickly generate dictionary files, word lists, or every possible combination of letters, numbers, and special characters and then attempt to log on
- Prevention; maximum number of login attempts on a system before the account is locked.

Performing Automated Password Guessing

- Guessing of a password, hackers use automated tools.
- use the Windows shell commands based on the standard NET USE (connect, disconnect, current status)syntax.

- Simple automated password-guessing script
- 1. Create a simple username and password file using Windows Notepad.
  Automated tools such as the Dictionary Generator are available to create this word list.
  Save the file on the C: drive as credentials.txt.
- 2. Pipe this file using the FOR command:
  C:\> FOR /F "token=1, 2*" %i in (credentials.txt)
- 3. Type net use \\targetIP\IPC$ %i /u: %j
  to use the credentials.txt file
  to attempt to log on to the target system's hidden share.

Defending Against Password Guessing

- Smart cards and biometrics add a layer of security to the insecurity that's inherent when users create their own passwords.
- A user can also be authenticated and validated using *biometrics*.
  Both smart cards and biometrics use *two-factor authentication,*

Offline Attack

TABLE 4.1 Offline attacks

Type of attack	Characteristics	Example password
Dictionary attack	Attempts to use passwords from a list of dictionary words	Administrator
Hybrid attack	Substitutes numbers of symbols for password characters	Adm1n1strator
Brute-force attack	Tries all possible combinations of letters, numbers, and special characters	Ms!tr245@F5a

Dictionary Attack

- simplest and quickest type of attack.
- It's used to identify a password that is an actual word, which can be found in a dictionary.

  the attack uses a dictionary file of possible words, which is hashed using the same algorithm used by the authentication process.

  hashed dictionary words are compared with hashed passwords as the user logs on, or with passwords stored in a file on the server.
- The dictionary attack works only if the password is an actual dictionary word;
- can't be used against strong passwords containing numbers or other symbols.

Hybrid Attack

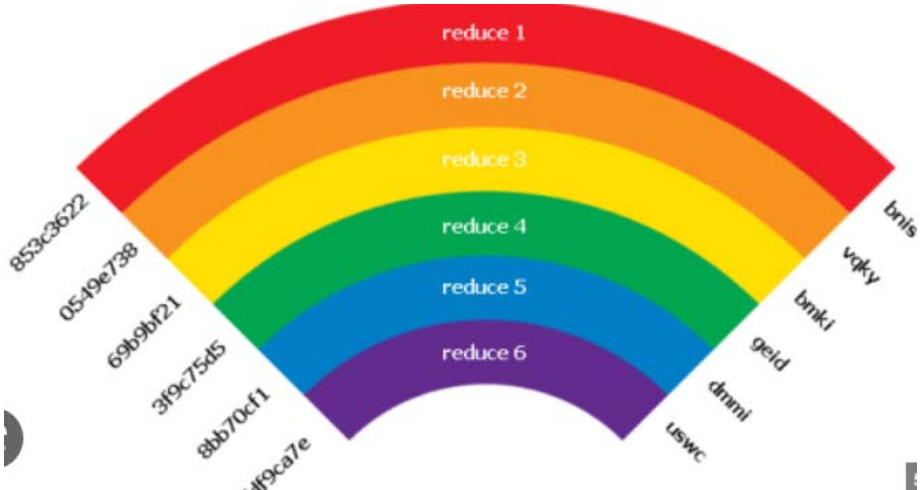
- if the password can't be found using a dictionary attack.
- The hybrid attack starts with a dictionary file
- Substitutes numbers and symbols for characters in the password.
- many users add the number 1 to the end of their password to meet strong password requirements.
- find those types of anomalies in passwords.

Bruteforce Attack

- most time-consuming
- which tries every possible combination
- of uppercase and lowercase letters, numbers, and symbols.
- slowest of the three types of attacks -many possible combinations-of characters in the password.
- However, brute force is effective;
- given enough time and processing power, all passwords can eventually be identified.

Rainbow Table

- A *rainbow table is a list of dictionary words that have already been hashed.*
- Rainbow tables can speed up the discovery and cracking of passwords by pre-computing the hashes for common strings of characters. For example,
- a rainbow table can include characters from a to z or A to Z.
- Essentially, rainbow table tools are hash crackers.
- The idea of rainbow tables is to do all cracking-time computation in advance.



Non electronic Attack

- do not employ any technical knowledge.

- social engineering,
- shoulder surfing,
- keyboard sniffing,
- dumpster diving.

- best defense-social engineering - is security-awareness training for all employees
- security procedures for resetting passwords.

- shoulder surfing,:
- Special screens that make it difficult to see the computer screen from an angle can cut down on shoulder surfing.
- In addition, employee awareness and training can virtually eliminate

Cracking a password

- Manual password cracking involves attempting to log on with different passwords.
    1. Find a valid user account (such as Administrator or Guest).
    2. Create a list of possible passwords.
    3. Rank the passwords from high to low probability.
    4. Key in each password.
    5. Try again until a successful password is found.
- A hacker can also create a script file that tries each password in a list.

A more efficient way of cracking a password is to gain access to the password file on a system.

- Most systems *hash (one-way encrypt) a password for storage on a system.*

- *During* the logon process, the password -is hashed using the same algorithm -compared to the hashed passwords stored in the file.
- A hacker can attempt to gain access to the hashing algorithm stored on the server instead of trying to guess

Passwords are stored in the Security Accounts Manager (SAM) file on a Windows system and in a password shadow file on a Linux system.

LAN Manager Hash

- Windows 2000 uses NT LAN Manager (NTLM) hashing - secure passwords in transit on network.
- Depending on the password, NTLM hashing can be weak and easy to break.

- let's say that the password is 123456abcdef.

When this password is encrypted with the NTLM algorithm,

- first converted to all uppercase: 123456ABCDEF.

- The password is padded with null (blank) characters- 14 characters long: 123456ABCDEF__.

- Before - encrypted, the 14-character string is split in half: 123456A and BCDEF__.

- Each string is individually encrypted, and the results are concatenated:
  123456A = 6BF11E04AFAB197F
  BCDEF__ = F1E9FFDCC75575B15

- The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15.

Cracking Windows 2000 Passwords

- The SAM file in Windows contains the usernames and hashed passwords.
- located in the Windows\system32\config directory.
- The file is locked when the operating system is running
- hacker can't attempt to copy the file while the machine is booted to Windows.

- One option for copying the SAM file is to boot to an alternate operating system -DOS or Linux with a boot CD.
- Alternately, the file can be copied from the repair directory.

- If a system administrator uses the RDISK feature of Windows to back up the system, then a compressed copy of the SAM file called SAM._ is created in C:\windows\repair.

- expand this file, use the following command at the command prompt:
- C:\>expand sam._ sam
- After the file is uncompressed, a dictionary, hybrid, or brute-force attack can be run against the SAM file using a tool like L0phtCrack.

Redirecting the SMB logon to the attacker

- To discover passwords- network is to redirect the Server Message Block (SMB) logon to an attacker's computer so that the passwords are sent to the hacker.

- So, the hacker must sniff the NTLM responses from the authentication server and trick the victim into attempting Windows authentication with the attacker's computer.

- Common technique is to send the victim an email message with an embedded link to a fraudulent SMB server.
- When the link is clicked, the user unwittingly sends their credentials over the network.

Redirecting the SMB logon to the attacker

SMBRelay

- An SMB server that captures usernames and password hashes from incoming SMB traffic. SMBRelay can also perform man-in-the-middle (MITM) attacks.

SMBRelay2

- Similar to SMBRelay but uses NetBIOS names instead of IP addresses to capture usernames and passwords.

pwdump2

- A program that extracts the password hashes from a SAM file on a Windows system. The extracted password hashes can then be run through L0phtCrack to break the passwords.

Samdump

- Another program that extracts NTLM hashed passwords from a SAM file.

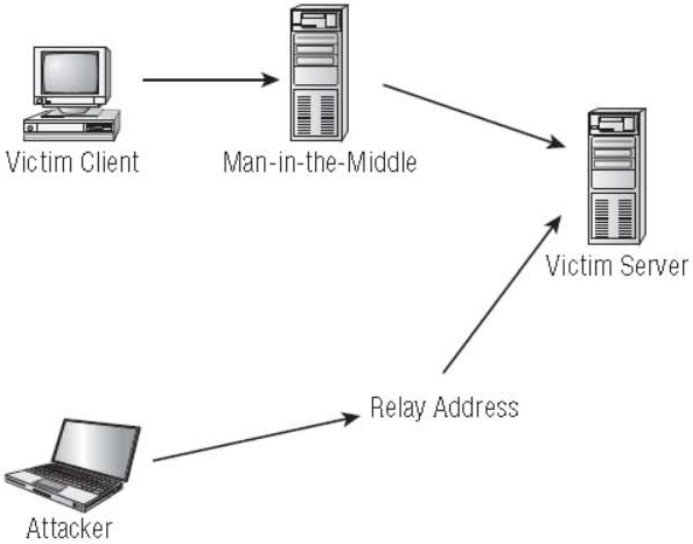
C2MYAZZ

- A spyware program that makes Windows clients send their passwords as clear text. It displays usernames and their passwords as users attach to server resources.

SMB relay MITM Attack

An SMB relay MITM attack is when the attacker sets up a fraudulent server with a relay address. When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password, and passes the connection to the victim server. Figure 4.1 illustrates such an attack.

FIGURE 4.1 SMB relay MITM attack



SMB relay countermeasures

- SMB relay countermeasures include configuring Windows 2000 to use
- SMB signing, which causes it to cryptographically sign each block of SMB communications..

NetBIOS DoS Attack

- sends a NetBIOS Name Release message to the NetBIOS Name Service on a target Windows systems and
- forces the system to place its name in conflict so that the name can no longer be used.
- This essentially blocks the client from participating in the NetBIOS network and creates a network DoS for that system.

Another way to create a more secure and memorable password is to follow a repeatable pattern, which will enable to password to be re-created when needed.

1. Start with a memorable phrase, such as

   Maryhadalittlelamb

2. Change every other character to uppercase, resulting in

   MaRyHaDaLiTtLeLaMb

3. Change a to @ and i to 1 to yield

   M@RyH@D@L1TtLeL@Mb

4. Drop every other pair to result in a secure repeatable password or

   M@H@L1LeMb

Now you have a password that meets all the requirements, yet can be "remade" if necessary.

Password cracking countermeasures

- To protect against cracking of the hashing algorithm for passwords stored on the server,
- you must take care to physically isolate and protect the server.
- The system administrator can use the SYSKEY utility in Windows to further protect hashes stored on the server's hard disk.
- The server logs should also be monitored for brute-force attacks on user accounts..

A system administrator can implement the following security precautions to decrease the effectiveness of a brute-force password-cracking attempt:

- Never leave a default password.
- Never use a password that can be found in a dictionary.
- Never use a password related to the hostname, domain name, or anything else that can be found with Whois.
- Never use a password related to your hobbies, pets, relatives, or date of birth.
- As a last resort, use a word that has more than 21 characters from a dictionary as a password.

Counter Measures

- **Password change interval:**
- **Monitoring Event Viewer Logs:**

Keyloggers

- Hardware
- Software: Software keyloggers
- can be deployed on a system by Trojans or viruses.