Techniques and Tools for Password Attack

P. S. Lokhande[1] B. B. Meshram[2]
[1]Assistant Professor [2]Professor
[1,2]Department of Computer Engineering
[1]AIKTC, Navimumbai [2]VJTI, Matunga, Mumbai

Abstract— Across the World Wide Web, the use of various online services and applications has increased drastically; password is the common and widely used method to validate the access to online applications. As usage of online application grows in sophistication and numbers, there is no doubt that virus creators, hackers, and organized criminals have started targeting them. Password authentication is the first line of defence against the unauthorised access, if attacker can breach those defences, he will get full control of the application and full access to the data. Attackers find it easy to attack online application by cracking password; to crack the password various techniques and tools are used. Some of the tools are available free on the internet. This paper will focus at various design and implementation flaws that commonly affect web applications authentication, and suggesting defence strategy to deal with password attack one by getting the knowledge of techniques and tools used for password cracking.

Key words: Password, User Authentication, Password Cracking, Brute Force Attack, Password Cracking tools, Attack on authentication

I. INTRODUCTION

This paper will highlight the key techniques and tools being used by the hacker's, and will put light on how these tools and the techniques are changing. Also focusing on various design and implementation loop holes that create web application vulnerable for authentication attack. Password is secret word that gives access to certain application. Password contains the sequence or words, characters, special characters and numbers as decided by user. Password gives protection to the online web application from the outer world, only legitimate user can access the data.

A. What is Password?

A password is a combination of un-spaced word of characters used to prove that user requesting access to a computer system is really legitimate user. A password may be combination of characters between four and 16 characters, depending on how the web application is designed. When a password is provided, the web application login system is designed not to display the characters on the display screen; generally it is represented by asterisks [1].

B. How the Passwords are Stored?

1) Plain Text Passwords :
The simplest way an online web application can store password in plain text on the web server, there exists a database with username and password in it in a human-readable form (Ex. if your password is test123, it is stored in the database as test123). When user enters his user id and password on the site, it checks in the database to see if they match. This is not recommended method, and most reputable web sites never store passwords in plain text. If someone gets access to this database, everyone's password is compromised.

2) Basic Level Password Encryption:
To give more protection to user password than plain text provides; most web sites encrypt user password before storing it on web servers. Encryption uses a special key to convert user password into a random string of text. It is difficult for hacker to gain the access in to user account unless they have the key, which they can use to decrypt it. The problem in this method is the key normally stored on the same web server that the passwords are, so in case servers get hacked, it will be quite easy job for hacker to decrypt all the passwords, which means this method is still insecure.

3) Hashed Passwords:
Hashing is similar to encryption it turn user password into a long string of letters and numbers to keep it hidden. However, unlike encryption, hashing is a one way road: If you have the hash password, then there is no way to get the original password. This means a hacker would have to obtain the hashes and then try a number of different password combinations to see which ones worked.

4) Hashed Passwords with a Dash of Salt:
Salting a hashed password means adding a random string of characters called a "salt" to the starting or end of user password before hashing it. This method uses a different salt for each password, and even if the salts are stored on the same servers, it will make it very difficult to find those salted hashes in the rainbow tables, since each one is long, complex, and unique.

5) Slow Hashes:
Many security experts looking to slower hashes as the most suitable option for storing passwords. MD5, SHA-1, and SHA-256 hash functions are relatively fast; if user type in a password, it will return the results fairly quickly. In a brute force attack technique, time is the important factor. By using a slower hash like the becrypt algorithm brute force attacks takes longer time, since each password takes more time to compute [4].

C. Password Authentication Techniques:

Various web based techniques are used in password authentication, every technique is having their own advantage and disadvantage. Some of the Password Authentication Techniques are given as follows.

1) HTML form based authentication:
This technique is very common and widely used authentication technique in the web forms. A HTML code is written to accept the used credentials.

2) Multifactor Authentication Mechanism:
To grant the access to the particular application used need to provide password as well some token number of generated by web application and delivered on the customers mobile number. This technique widely used by the banks.

3) Client SSL Certificates:

A client certificate contain information like a digital signature, SSL/TLS version number , serial number, expiration date, name of client, name of CA (Certificate Authority), revocation status, which is structured using the X.509 standard.

At the start of a Client SSL session, the server requires the client application to submit a client certificate for authentication. After receiving the certificate, the server uses it to identify the certificate's source and determine whether the client should be allowed access [5].

4) HTTP Basic and digest authentication:

Digest Authentication communicates user ID and password in an encrypted form by adding a hash function to the username, the password, a server supplied nonce value. Basic Authentication uses unencrypted base64 encoding.

5) Windows integrated authentication using NTLM:

It uses the security features of Windows clients and servers. Unlike HTTP Basic or Digest authentication, initially, it does not prompt users for their credentials. The present Windows user information on the client computer is provided by the web browser through a cryptographic exchange involving hashing with the Web server. If the authentication exchange fails to identify the user, the web browser will prompt the user for a Windows user account user name and password [6].

II. ATTACKS ON PASSWORD

An attempt made to steal passwords using a password cracking tool is considered as password attack. Hackers widely use various password cracking tools available online and techniques to steal user data. Following are the types of the most widely used attacks.

1) Password Guessing: This is a very common type of attack, hackers can guess passwords locally or remotely using either a manual or automated approach. Many tools available to automate the process of typing password after password. Some common password guessing tools are Hydra [8] for guessing all sorts of passwords, including HTTP, Telnet, and Windows logons.
2) Password Resetting: Easier way to attackers to reset passwords than to guess them. Many password cracking programs are actually password resetters. Most password resetters contain a bootable version of Linux that can mount NTFS volumes and can help you locate and reset the Administrator's password. A widely used password reset tool is the free Petter Nordahl-Hagen program (http://home.eunet.no/~pnordahl/ntpasswd).
3) Winternals ERD Commander 2005, (http://www.winternals.com/Products/AdministratorsPak/#erdcommander2005)
4) Password Cracking: Password cracking method takes a copied password hash and converting it to plaintext original. For password cracking, an attacker uses tools like extractors for hash guessing, rainbow tables for looking up plaintext passwords, and password sniffers to extract authentication information.
5) Hash guessing: Some password cracking tools can both extract and crack password hashes. The widely used Windows password hash extractor is the Pwdump family of programs [7].
6) Rainbow tables: In this technique attacker is computing all possible passwords and their hashes in a given system and putting the results into a lookup table called a rainbow table. One can purchase very large rainbow tables, which vary in size from hundreds of megabytes to hundreds of gigabytes, or generate your own using Rainbow Crack [7].
7) Password sniffing: Password crackers can sniff authentication traffic between a client and server and extract password hashes or enough authentication information to begin the cracking process.
8) Tools password crackers are using are ScoopLM (http://www.securityfriday.com/tools/ScoopLM.html) and
9) KerbCrack (http://ntsecurity.nu/toolbox/kerbcrack), Password Capturing : In this technique attackers capture passwords simply by installing a keyboard-sniffing Trojan horse or one of the many physical keyboard-logging hardware devices for sale on the Internet.

A. Password Cracking Tools:

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It recovers various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort. It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources, however it also ships some "non standard" utilities for Microsoft Windows users.

B. Corrective Measure to Secure Password:

Prevention is better policy than to face the situation, if web developer and user of the system can take following corrective measures at designing phase then there is a chance to avoid the situation like the password cracking.

Don't use services with bad security. You are not aware about the service given by the company, how they are storing your password, suggested way is user should never sign up for a service that uses plain text or encryption to store theirr passwords, because these passwords are much more vulnerable to being compromised. Best way find out what service provider use, click the "lost password" link. If it sends user password in an email, that means they can access the password itself and it isn't hashed and it's likely stored using one of the less secure methods.

Use a strong password: Stronger user password has less chances to crack.. Length is more important than complexity. Keep in mind any password is crackable, you just want it to take as long as possible.

Always change your password after few days: It is applicable for the strong password too, Those with weak passwords may have already had their account compromised by the time they realize the leak has happened, but user password takes days to crack, then they have time to change it and make their old password useless by the time they figure it out.

Use a different password for every site: Habit of using different password for every account, then those accounts will stay safe even if one of accounts gets compromised. If the same password is used for every site, one site's breach can mean a whole accounts may be in trouble.

User can use OAuth if its unsure about a site's security: OAuth, the protocol helps user log in using their Google, Facebook, or Twitter account. Google, Facebook, and Twitter are likely to have better security, and if the site is breached, user can just revoke its access from Google, Facebook or Twitter account.

C. Guidelines to choose good password [1]:

- Good criteria when choosing a password or setting up password guidelines includes the following:
- Don't pick a password that someone can easily guess if they know who you are (for example, not your Social Security number, birthday, or maiden name)
- Don't pick a word that can be found in the dictionary (since there are programs that can rapidly try every word in the dictionary!)
- Don't pick a word that is currently newsworthy
- Don't pick a password that is similar to your previous password
- Do pick a mixture of letters and at least one number
- Do pick a word that you can easily remember

III. Design Flaws in Authentication Mechanism

A. Bad Passwords:

- Short or Blank password
- Dictionary Words
- Similar to username
- Date of birth
- Mobile Number

B. Brute Forcible Login:

Burp Intruder Tool : Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities [3]
Countermeasures: Client side controls to prevent password guessing attacks.

C. Vulnerable Transmission of Credentials:

An application that uses unencrypted HTTP to transmit login credentials an eavesdropper who is positioned on the network can intercept it.

D. Places:

- Users local network
- Users IT dept
- Within Users ISP
- On the internet backbone

E. Password Change functionality:

Improper password change functionality may result in cracking the account by cracker who knows some information about the user.

F. Forgotten Password Functionality:

This functionality should have the stronger validation and security check mechanism.

G. Remember Me Functionality At Login:

This functionality feature allows unattended desktop/ laptop vulnerable to cracker to access in to account and change the password.

H. User Impersonation Functionality:

Care should be taken while giving the privilege of impersonating user.

I. Non Unique Usernames for Login:

Constraint should be defined to have a unique user name for log in.

J. Password Policy:

Define validation mechanism at the time of user registration for setting password such as One upper case word, one special character, one special character and length of password should not be less than 6 characters and greater than 16 characters.

IV. Conclusion

Password is the gateway to access the user information, a first level defence mechanism. With the growth of www web all transaction are done on web, which attracts the criminals to earn easy money with minimum risk of being captured. Day by day attackers are committing various attacks on the online application, they are using various automated online tools to hack the user account. This paper focuses on the various tools their way of cracking the password; this study of the modus of operandi will help the user to design the web application in a way to make their first level of defence strong. Knowledge of the available tools is used to pen test the application in design stage. Design flaws at the authentication mechanism should be rectified at the application design level.

References

[1] Margaret Rouse, “Password”, available online: http://searchsecurity.techtarget.com/definition/password
[2] Dafydd Stuttard, Marcus Pinto, “The Web Application Hackers Handbook”, Finding and Exploiting Security Flaws, 2nd Edition, Wiley Publication, ISBN:978-81-265-3340-4, 2015.
[3] Burp Suite, Available online:
[4] Bcrypt algorithm: https://en.wikipedia.org/wiki/Bcrypt
[5] Client SSL Certificate: http://www.jscape.com/blog/client-certificate-authentication
[6] Integrated windows authentication: https://en.wikipedia.org/wiki/Integrated_Windows_Authentication
[7] Lokhande, P. S., and B. B. Meshram. "E-Commerce Applications: Vulnerabilities, Attacks and

Countermeasures." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.

[8] Hydra: Web Link: http://www.thc.org/blob/manhydra/thc_hydra_article_r3.pdf

