AN OVERVIEW OF HACKING TECHNIQUES AND METHODS TO PREVENT IT

Abhay K.Kolhe
Dept. Of Computer Engineering
MPSTME, NMIMS University
Mumbai, India
kolhe.abhay@gmail.com

Pratik Adhikari
Dept. Of Computer Engineering
MPSTME, NMIMS University
Mumbai, India
prtkadhikari@gmail.com

Abstract— Security has become one of the most important goals in this era. Well there is no game in the rule of hacking .In this paper we will describe the various methods used for bypassing authentication credentials. We will also provide list of some software's for windows environment (freeware which cannot be guaranteed) for educational purpose only to get authentication credentials. The Paper mainly focus on the sql injection attacks, use of key- loggers to bypass authentication credentials and hacking in windows environment by bypassing SAM databases and way to prevent these types of attack.

Keywords:magic-strings,keyloggers,hacking,windows,SAM, Skype.

I. INTRODUCTION

In the recent trend hacking the system have become the childs plays with the automated software's like havij,sql mapper, Zenmap,wireshark,keyloggers.In this paper we are providing an overview on how the attacks can be done and mechanism can be made to prevent it. Well there are many attacking techniques that can be done for exploiting vulnerabilities; we would like to focus only few of them.

Security is always topmost priority concern for any organization. Attackers use various techniques to attack the system without any rules and regulations. So it's always a burden on the victim site to prevent the attacker's attacks by different methods. No system can guarantee a full proof protection mechanism. There are many techniques to exploit vulnerabilities in the system such as Setting Backdoor in Windows Trojan horse, session hijacking, website defacement, email bombing and spamming, cross side scripting, denial of service, phishing etc.

A) SQL injection attacks:

The sql injection generally fools the database as a regular query by the user and gets accessed to the system easily. Most of the websites are hacked by sql injections itself [1].

There are different types of sql vulnerabilities.

a) Incorrectly filtered escape characters:

There are times by the developer when sql statements are not filtered for escape characters, then this form of sql injection takes place [1].

Let us take the examples:-

Statement = "SELECT * FROM customers WHERE name = '" + customerName + "';"

If customerName is replaced by sql string like 'x'=x during authentication, the database responds to the code in the usual manner as the first one that is used to display records.

b) Incorrect type handling

There are the times when developers forget to provide strongly typed constraints.

"SELECT * FROM data WHERE customer_id = " + variable + ";"

The developers or programmer makes no checks to validate that the user supplied input is numeric. This would be able to replace "variable" very easily by any data types.

For e.g:- 1; DROP TABLE Customers.It will delete (DROP) the "Customers " table from the database. The formatter will need to create these components, incorporating the applicable criteria that follow.

Magic string: It is the strings that we used to get login in the pages as the authenticated users. The magic string is 'OR''=' [1].

c) Blind SQL injection

In this type of attacks web page are vulnerable to attacks but the results are no visible to the attackers.

SELECT Cust_name FROM Customer WHERE Cust_Id = ‘125’ AND 1=1

The above statement will result in a normal page while SELECT Cust_name FROM Customer WHERE Cust_Id = ‘125’ AND 1=2 will likely give a different result if the page is vulnerable to a SQL injection. Attackers keep on modifying these values until they get useful information. These statements helps the attacker to know if blind sql injection is possible or not, then the attacker will devise statements that will evaluate to true or false depending on the contents of a field in another table [1].

i) Conditional Errors

SELECT 1/0 FROM Customers WHERE Cust_id=’125’ .It returns error only when where condition is true The division by zero will only be evaluated and result in an error if Customer 125 exist[1].

ii) Time Delay

Based on the time taken to execute query attackers get some hint weather the injected statement is true or not.

NOTE:

Before moving further we want our readers to know that doing malicious activity is not legal ,you can penalized to fine or even to jail in some countries. Below we are providing list of commonly used query for sql injections and attacks that can be used in vulnerable websites.

SOME COMMONLY USED SQL ATTACKS:

' or '1'='1
' or '1'='1' - - '
' or '1'='1' ({ '
' or '1'='1' /* ' [12].

B*) Automated Software that is used:*

SQLMAP: Sql map is open source software which automates the process of detecting and exploiting sql injections flaws. It has a powerful detection engine, it can be used by the both beginners and experts. It has broad range of switches used for database fingerprinting, fetching the data from database, to access the underlying file system. Sql map requires python version 2.6x or 2.7x [2].

ZAPROXY: Wells it’s a penetration testing application supports wide variety of applications including sql injections, port scanning. The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing. Zed Attack Proxy provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually [3].

HAVIJ: It’s easy to use software. No knowledge about programming language is required to use this software. Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page. It can take advantage of a vulnerable web application. By using this software user can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetching data from the database, running SQL statements and even accessing the underlying file system and executing commands on the operating system. The power of Havij that makes it different from similar tools is its injection methods. The user friendly GUI of Havij and automated settings detections makes it easy to use for everyone, even amateur users [4].

C) Prevention methods provided for sql injections attacks:

a) Interpret at web server level

Mod-security is an open source firewall that can be installed in the server level. It is based on the keyword specification. Whenever the keyword specifying the particular attack is matched, it informs the server about this and generates an error. It removes multi forward and slashes and self referenced directories, treating forward and backward slashes equally, decoding URL and replacing null bytes [1].

b) To interpret at language level

We escape characters in php by replacing a single quote (‘) in a parameter by double quote to make it a valid SQL statement. Web developers regularly use mysql_real_escape_string() function for escaping special characters. It adds backslashes to characters \x00, \n, \r, \, ', and \x1a before sending the query to MySQL. So it will help the server to determine whether the query is valid or it’s an attack from the attacker’s side [1].

c) To interpret with SQL firewall

SQL injection can be prevented to some extent by using GreenSQL, which is an Open Source database firewall that works as a proxy and inbuilt MySQL support. It blocks Db administrative commands and uses risk scoring matrix to analyze commands [1].

d) User Privileges

The admin rights should be divided and the concept of one admin who can delete, create, edit and modify table should be avoided [1].

e) Encrypting Data

Data can be encrypted in separate table or a separate server to provide extra security from the attackers. The choice of the encrypting algorithm should be efficient and intelligent [1].

II. *Using Keyloggers to get authentication credentials*

Well keyloggers are extremely powerful devices that are used to get authentication credentials of the user with an ease. Mostly key-loggers record the strokes in the key boards once it's installed in the victim's device. There is even no need to decrypt the authentication credentials when some strong keyloggers are used .There two types of keyloggers used:

a) Hardware keyloggers: Hardware keyloggers is mainly the electronic device used for capturing the keystrokes of the key board. There are many hardware keyloggers available in the markets that can be plugged in the connecting interface between CPU and the keyboard. The main advantage of the hardware key-loggers is that it's not detected by the antivirus software's. For e.g. Keyghost is the company making hardware keyloggers [6].

b) Software keyloggers: Software keyloggers record the keystrokes within the target operating system. It stores the data in the hard-disk or in some remote locations. The main flaw of the software keyloggers is that it is easily detectable by antivirus and it can't be used when user uses the virtual key board which is operated by the mouse clicks [5].

A) Prevention method provided for keyloggers

The process involves three things mainly
Original Password: The password which is used in trusted systems.
Fabricated Password: The password used in un-trusted systems.
Pen -drive/ unique id: This is the key used for identification of the Hardware Device [5].

The main concept used in this method is to take the required input and to generate the fabricated password that can be used in the untrusted environment. The application also needs to store the key along with the codes required for the activation of the Temporary filter layer (TFL) on USB.USB storage device is having key and TFL needs to be connected in the un-trusted machine. Once it gets connected its automatically gets started. As soon as the password is entered through the keyboard the pressed key goes to the operating system and then the keyboard driver of the operating system translates those keystrokes into a Windows message called WM_KEYDOWN. This message is pushed into the system message queue. The operating system in turn puts this message into the message queue of the thread of the application related to the active window on the screen. The thread polling queue sends the message to the window procedure of the active window [5].

III. *Hacking in the windows environment*:-

Windows uses md5 and rc4 to encrypt the password. In windows ME password are stored in the password list (.pwl). We can go to c:\windows folder and find the *.pwl files using operating system find option .These .pwl file are readable but not understandable.

SAM databases: System Accounts Manager is implemented as registry file to store the password. To use the SAM root key handle is used HKEY_LOCAL_MACHINE (HKLM).
The SAM is stored in the location:
%SystemRoot%\System32\config

SAM registry file is locked when operating system is running. So we can change and modify it during the booting time [7].

A) Password Storage Mechanism for different applications in windows environment

a) Internet Explorer

Internet explorer stores password in encrypted form in the secure location known as 'protected storage' at following registry location [7].

HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider
Internet Explorer 7 stored along hash of website URL in the storage location:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

b) Google talk:

GTalk stores all remembered account information at following registry location [7].
HKEY_CURRENT_USER\Software\Google\Google Talk\Accounts

c) Skype

The mechanism of storing the password by the Skype is not direct. It computes the encrypted hash of the password and stores in config.xml present in the Skype's user profile directory [7].

For Windows XP
C:\Documents and Settings\<user_name>\Application Data\Skype\<account_name>

For Windows Vista & Windows 7
C:\Users\<username>\AppData\Roaming\Skype\<account_name>

B) Method used:
Step 1: Login to a Computer that has Windows XP system.
Step 2: Copy the SAM file to a floppy disk.
Step 3: Then turn to your locked pc and insert the floppy disk Reboot the PC and enter into MS-DOS.
Step 4:In dos,type : del c: windowssystem32configsam ,then you will delete the SAM file.
Step 5: type: Copy a: sam c: windowssystem32config,copy the other's SAM file to your PC[7].

C) Software's available

a) Ophcrack: is a free Windows password cracker based on rainbow tables. A rainbow table is a pre-computed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password, up to a certain length consisting of a limited set of characters [13]. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms. Windows 2000, XP, Vista and 7 are supported [8].

b) LophtCrack: is a Security Assessment tool that can be used for password auditing and recovery [9].

c) Offline NT Password & Registry Editor: Offline NT Password & Registry Editor works differently than most password recovery programs in that it erases your Windows password instead of recovering it. You can think of it as more of a Windows password reset tool[10].
There are many more password crackers available. You can use it on your own risk. These all methods and tools are given just for educational purpose.

*D) How to prevent attacks on SAM database***?**

a) Disabling the NT Scheduler service: The trick involves using the NT Scheduler service to start the Registry editor and scheduling regedt32.exe to launch on the desktop at some predetermined time. By default, NT Scheduler runs under the user security context of the SYSTEM account. Thus, any program NT Scheduler launches has full system authority, including full access to the SAM database. Guarding against this risk is tough because you need to disable the service. Disabling NT Scheduler isn't always possible because a given system might require the service for routine tasks. If you can't disable the NT Scheduler service, consider configuring it to run under the user context of a user with only enough authority to perform any scheduled actions [11].

b) Using system key technology: Additionally, you can employ Microsoft's system key technology to further protect the SAM. This technology made its first appearance as part of a post-Service Pack 2 (SP2) hot-fix, but system key technology made a bigger splash in SP3. In a nutshell, system key technology helps protect NT and its passwords by encrypting the SAM database and requiring the use of an encryption key to boot the operating system [11].

CONCLUSION:

In the recent years security have been top most priority of any organization .We heard many news that many secured websites have been hacked by the juvenile hackers. This paper deals with the methods to strengthen our security and make hackers job difficult to hack any system. Although we never say that system will be 100% secured by applying these techniques but it will make hackers work difficult. We have also discussed about various automated tools which can make anyone with a little programming knowledge to penetrate the systems and applications. Real hacking and cracking requires lots of skill and dedication. Future work we will focus on finding vulnerability on windows 7 and 8 also we would like to provide more effective way to prevent sql injection attacks.

REFRENCES

[1]Ramakanth Dorai,Vinod Kannan, "SQL Injection-Database Attack Revolution and Prevention" ,Journal of International Commercial Law and TechnologyVol6, Issue 4 (2011)
[2] http://sqlmap.org 28th Jan 2013
[3] http://code.google.com/p/zaproxy/ 28th Jan 2013
[4]http://www.itsecteam.com/products/havij-v116-advanced-sql-injection/ 28th Jan 2013
[5]Nairit Adhikary1, Rohit Shrivastava2, Ashwani Kumar3, Sunil Kumar Verma4, Monark Bag5, Vrijendra Singh 6, "Battering Keyloggers and Screen Recording" Software by Fabricating Passwords, 2012
[6] http://www.keyghost.com 28th Jan 2013
[7]C.K. GOEL and GAURAV ARYA,"Hacking of Passwords in Windows Environment", 2012
[8]http://ophcrack.sourceforge.net/ 28th Jan 2013
[9] www.l0phtcrack.com 28th Jan 2013
[10]http://pcsupport.about.com/od/toolsofthetrade/tp/passrecovery.htm 28th Jan 2013
[11]http://technet.microsoft.com/en-us/library/cc723740.aspx 28th Jan 2013
[12] http://en.wikipedia.org/wiki/SQL_injection 28th Jan 2013
[13]http://en.wikipedia.org/wiki/Rainbow_table 18th sep 2013