IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

SYSTEM SECURITY AND ETHICAL HACKING

Kumar Utkarsh

Computer Science & Engineering
Dhanalakshmi Srinivasan College of Engineering & Tech,
Mamallapuram, Chennai-603104 (India)

Abstract

We are living in security era, where we are securing all our belongings under different modes of lock but it's different in the case of system security. We are carelessly leaving our datas and softwares unlocked. The main motive of this paper is to make aware of different types of hacking tricks by which a hacker can hack and destroy our precious datas as well as the tricks & suggestion to prevent our system to be hacked.

I. INTRODUCTION

Security is a discipline which protects the confidentiality, Integrity & availability of resources. I refer this era as a "security Era" not because we are very much concerned about security but due to the maximum need of security in this era, thieves are waiting when we make mistake and they steal our information. Today we are securing all our precious items with high tech security but most of us are least concerned about the security of system and data in it.

II. SECURITY TYPES

Broadly we can divide security in three divisions

1.System security
2.Data Security
3.Network Security

System security is least consider nowadays also when we have maximum number of hackers and crackers.

III.SYSTEM SECURITY

System security means securing a system from unauthorized access by the person who can physically access it.System security is further divided into two divisions

1. Data accessible restriction
2. System accessible restriction

A. Data Accessible Security

When we give permission to a user to access only certain files and folders in a system then it is consider as the Data Accessible Security.We can achieve data accessible security by many ways.Some the ways are:-

1) Encrypting Hard disk: We can use encrypting softwares and encrypt the entire hard disk and store the personal information, which we don't want to share with others.

2) Hiding Folders: We can hide the folder from the user. But it is not very secured method, unauthorized person with little computer knowledge can also easily access the hidden folders or files.

3) *By locking folders:* We can simply lock the folders which we want to be personal. We can also lock entire hard disk. When a folder is lock, it will not appear in the search also. Even it's impossible to access it in DOS mode. So the document is well protected. In my view, The best software for folder locking is FolderLock7.

Fig. 1 Screen shot of Folder Lock7

a. KEYLOGGERS

Keyloggers are a software or hardware which records the screenshots or keystrokes without the knowledge of user.

Types of keyloggers:

1.SOFTWARE KEYLOGGERS

Software keyloggers are a software which records screenshots and keystrokes etc. and create a log file of all these details and send it to the hacker's email.some of the software keyloggers are password protected also, which make very difficult to detect and disable them.

2.HARDWARE KEYLOGGERS

Hardware keyloggers are a hardware which is attached at the port of keyboard and records all the keystrokes in the in-built memory.It comes in two types of port:

i)PS/2
ii)USB

b. ANTI KEYLOGGERS

Hardware key loggers can be detected by carefully observing the port but to prevent system from software keyloggers, we need to install anti keyloggers.It works similar to Anti viruses which stop virus softwares where as anti keyloggers stop keyloggers software.

Fig.2 hardware keylogger

B. System Accessible Security

System accessible restriction means restricting someone to access the system completely, it can be refered as OS level security.The easiest way is to:-

i) Provide user password in the system

IV.SAM(SECURITY ACCOUNT MANAGER)

SAM stands for security account manager. It is a registry file which holds the value of user login details (user name & password) in a hash table which when matched with the user entered details, redirect to the desktop of the corresponding user. It works similar to our facebook login which redirects the user to the home page of the facebook when the correct user name and password is found in the database.

V. CRACK FOR WINDOWS XP

A. LOGIN

Usually while installing XP, the installer doesn't give any password in the administrator field and after installing we create our user accounts with password so the administrator remains without password.

When we start the windows, welcome screen ask for password just press CTRL+ALT+DEL and the screen will change to old windows login and in username write administrator and leave the password field blank and press ok, you will login to the desktop .

Fig.3 Old login screen

B. Changing Password of other users

We can change the password of other users also by simply writing following command in DOS mode

C:\Net user username password

But for doing that we need to have admin right in that particular system and we can change the password of other admin users.

VI. KON BOOT (UNDEFENDABLE HACKING SOFTWARE

If these methods fail then we can use KON BOOT by which we can crack any version of Windows & Mac passwords. Simply make the pen drive bootable with kon boot by the help of boot usb software. Boot from pen drive and follow the instructions. It works by overcoming the Sam file and directly login to the system.

fig.4 screenshot of KON BOOT V2

VII. PROTECTION USING SYSKEY

SYSKEY is a feature which is available in the Windows OS from WIN NT onwards, which give the facility to store the SYSKEY in a removable media so that unauthorised accessed can be prevented, without inserting the same media we can't access the particular system.It will work similar to a key of a lock without which you can't open the lock.

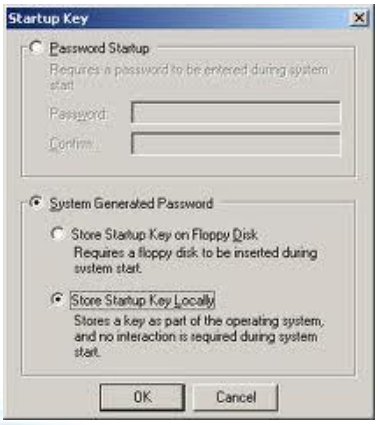

Fig.3 screenshot of SYSKEY

VIII. TIPS FOR SECURING SYSTEM DATA AND SYSTEM

- Install and Use Anti-Virus, firewalls & Anit key logger Programs
- While installing OS like Windows XP give admin password.
- Use Care When Reading Email with Attachments and following links.
- Install and Use a Firewall Program
- Make Backups of Important Files and Folders
- Use Strong Passwords and change it regularly as you change your toothbrush.
- Use Care When Downloading and Installing Programs
- Install and Use a Hardware Firewall
- Install and Use a File Encryption Program and Access Controls
- Safeguard your Data
- Real-World Warnings keep you safe online.
- Keeping Children Safe Online
- Use SYSKEY for password protection.

IX. CONCLUSION

We should pay maximum attention towards our system security and we can do the same by remembering this line "Treat your password like you treat your toothbrush. Never give it to anyone else to use, and change it every few months & most importantly use SYSKEY"

ACKNOWLEDGMENT

I acknowledge my deep sense of gratitude to my parents (Dr. Bipin Bihari Agrawal & Dr. Punam Agrawal) who encouraged me at every difficult turns and corners of my life without whom this paper was impossible to complete

.

I further extend my gratitude to my honourable Principal sir(Dr. R. Ponraj) & Head of department of CSE(Mr. N. Thulsi Raman) for allowing me to attend such events. I also thank SARASU mam (Assistant HOD of CSE) & Tamilarasi mam (Assistant Professor CSE) for boosting up my confidence as well as giving their valuable suggestions and feedbacks for my improvement.

At last but not the least I thank my friends Mr. Amit Kumar Pandit & Mr. Abhishek Anand for helping me with all sorts of resources to complete my paper.

References

[1] Internet
[2] Appin Technology lab "ethical hacking & information security" course material