International Journal of Power Control Signal and Computation(IJPCSC)
Vol3. No1. Jan-Mar 2012 ISSN: 0976-268X
www.ijcns.com

Ethical Hacking

Dinesh Babu S
Department of M.C.A, Adhiyamaan College Of Engineering
M G R Nagar, Hosur.
Anna University Coimbatore
Tamilnadu
India
dineshutg@gmail.com

Abstract

Hacking is one of the most dangerous disease from which the global world is suffering from. This project concentrates on how the malicious attacks and the effects of hacking caused to our community .It provides complete picture and preventive measures so solve the problem of hacking. Different aspects of hacking are discussed over here. Today's generation is still lagging in solving the problem of hacking attacks and in taking out the preventive measures in solving this global problem which is increasing day by day. To solve this problem of hacking attacks sophisticated security tool are invented. That's why we should start to think about hacker's psychology as the main way to prevent and stop attacks by understanding their needs or desires. The invention of internet has solved many problems and brought many new things to this world like electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, but at the same time it gave rise to the most dangerous problem called hacking. Governments companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. This study describes the skill, attitude and how this will help the customers finding and plugging security holes and the ethical hacking problem is explained and along with global problems and solutions to those problems are listed out.

Keywords **– Hackers, Internet, Governance, Expert regulation, Deliberative democracy**

1. INTRODUCTION

Hacking means to "gain unauthorized access (to data in a computer)". Banks defines hacking as "something that boring mainframe computer operators did to improve performance and battle boredom." [1]. Here a bank focuses on boredom as the reason of hacking. Darlington believes hacking is not limited to accessing data or information but also includes an attack on the privacy of all people [5]. Almost all different opinions agree on the illegality of hacking. On the other hand the word hacker is the agent of hack or hacking and it was defined as a person who enjoys accessing files whether for fun, imposing power or the interest related to the accessed files or data according to Taylor [9]. While Marotta has a negative view of the hacker as a data lord, a barbarian who takes what he wants [10]. Himanen defines hacker as any person who performs illegal actions whether they were related to computer or not which means the usage of a device apart from its functionality.

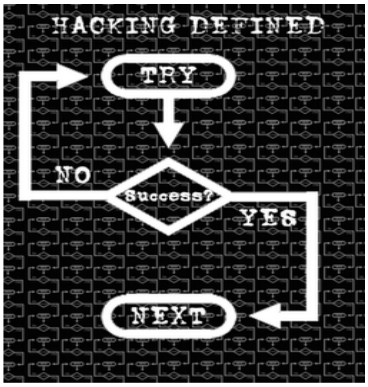


Figure.1 Ethical Hacking

A. Introduction to Hacking

"Hacking" is the word that shakes everyone whenever it is said or heard by someone. Everyone born in this world with attitude wants to be a Hacker. But it is not a job of a new born baby or an old grown lady. A Hacker needs a brilliant mind to hack anything. His skills should be so powerful that no other hacker can hack him. A Hacker doesn't need a software to hack. There are many rules that he should learn to become an Ethical Hacker. These rules include knowledge of HTML, JavaScript's, Computer Tricks, Cracking & Breaking etc.etc.

B. History of Hackers

Kevin Mitnick, often incorrectly called by many God of hackers, broke into the computer systems of the World's top technology and telecommunications companies Nokia, Fujitsu, Motorola, and Sun Micro systems. He was arrested by the FBI in 1995, but later released on parole in 2000. He never termed his activity hacking, instead he called it social engineer in November 2002 Englishman Gary

McKinnon was arrested in November 2002 following an accusation that he hacked into more than 90 US military computer systems in the UK. He is currently undergoing trial in a British court for a fast-track extradition to the US where he is a Wanted man. The next hearing in the case is slated for today.

C. Hacking Method

Phising Method- Phising is the method that you are familiar with. You create a Fake Account and ID in yahoo and fool your friends by telling them to send the victim's ID, their own ID and their own Password in your Fake Yahoo Account.

Brute Force Hack- Brute Force Hack is a Hacking which takes much time to get Password of the Victim and it needs a Hacker to learn about JavaScript's and all the non-sense. *Fake Login Hack*- Fake Login Hack is the Hacking used by most of you for your goal by creating a Fake Login Page and telling your friends to login there and the Password would come to you.

Cookie Steal Hack- Cookie Steal Hack is somewhat similar to Fake Login Hack as you prepare a Cookie Stealer and tell your friends to open your Cookie so that his Password would come to you.

Web Mail Hack- Web Mail Hack is the toughest method to learn for Hacking as it also needs a Hacker to learn about JavaScript's, Computer Tricks and much more and there is also a software for this type of Hack.

2. TYPES OF HACKING

White Hat Hacker- Also referred as Ethical Hacker or sometimes called as Sneakers. A White Hat Hacker mainly focuses on securing corporate Network from outsider threat. They are with good intention who fight against Black Hat.

Grey Hat Hacker- They are Skilled Hacker who sometimes act legally and sometime not. In simple word you may call a Grey Hat hacker as Hybrid between White Hat and BlackHathacker.

Black Hat Hacker- Also referred as Cracker. A Black Hat Hacker's intention is to break into others Network, and wish to secure his own machine. They often uses different techniques for breaking into systems which can involve advanced programming skills and social engineering.

3. HACKING WITH ETHICS

A. Hacking Websites

If you possess the HTML & JAVA knowledge then u can even access password protected websites. To hack a Password Protected Websites just follow these steps:

- Open the website u want to hack. Provide wrong username-password.(e.g : Username - me and Password - ' or 1=1 --)An error occurred saying wrong username-password. Now be prepared your work starts from here...
- Right click anywhere on that page go to view source.
- There u can see the html codings with JavaScript's.
- Before this login information copy your login the site in which you are.
- Then delete the java script from the above that validates your information in the server.(Do this very carefully, your success to hack the site depends upon this i.e how efficiently u delete the JavaScript's that validate your account information)then look for...code ..: input name="password" type="password"
- Replace there instead of . See there if maxlength of password is less than 11 then increase it to 11(e.g : if then write
- Just go to file => save as and save it any where with in the hard disk with ext.html(e.g :c:hack.htm)
- Close your webpage and go to the webpage u save in your hard disk(e.g : c:hack.htm) Open it.
- U see that some changes in current page as compared to original One. Don't worry.
- Provide any username[e.g:hacker] and password[e.g:' or 1=1 --]Congrats! you have cracked the above website and entered into the account of 1st user saved in the server's database.

B. Locally Stored Passwords

Most browsers, including Internet Explorer® and Netscape®, the AOL® client, and Windows® Dial-Up Connections allow you the option to store passwords. These passwords are stored on the local machine and (depending upon where and how it is stored) there is usually a method of recovering these passwords. Storing any password locally is insecure and may allow the password to be recovered by anyone who has access to the local machine. While we are not currently aware of any program to recover locally stored AOL® passwords, we do not recommend that these are secure. Software does exist that can recover most of the other types of locally stored passwords.

C. Trojan

A Trojan is a program that is sent to a user that allows an attacker to control functions of the target computer, recover information from the target or to delete or damage files on the target. The name Trojan is given because the program will usually come attached to some other program or file that entices you to run it. There are a wide variety of Trojans any number of which can be programmed to capture passwords as they are typed and to email or transmit them to a third party. To protect yourself against Trojans, you should never execute or download software or files that are not from

a trusted source. It is critical that anyone working on internet use a virus protection program (which should catch most Trojans.) Note that since a Trojan requires the password to be typed or stored in order to be recovered, this is not an effective way to recover your own password. It could explain, however, how someone could lose their password to a hacker. Sending someone a Trojan program is certainly illegal and we do not recommend or condone this activity. A Trojan is unlikely to be effective in recovering a particular account password since it requires the target to install it. However, hackers will often bulk mail Trojans to thousands of people in the hope that a small percentage will get caught. Legitimate account holders who may have been caught by a Trojan and can authenticate themselves should contact their service provider to have their account passwords reset.

D. Keylogger

A keylogger is a program or piece of hardware that records all keyboard keystrokes to an encrypted file which can then be read later. Based on the order of the keystrokes, it is usually easy to identify the password(s) from the file later. Like the Trojan, this also requires that someone actually type the password. Key loggers come in two types: hardware and software. A hardware keylogger can be fitted between the keyboard cable and the computer and can be activated with a few keystrokes. It is then left in place until after the password that you are looking to recover is typed. Later it is removed and the file of keystrokes is examined for the password. A hardware key logger is un deductable by anti-virus software.

A software key logger is installed on a system and effectively has the same function, however, it is a little bit more complex to use since it must be installed to run stealthily to be effective. A key logger could be used to steal a password from someone who is using an office computer or sharing a computer. It is possible that installing and using such a device or piece of software could be illegal depending upon whether the target has a presumption of privacy when using the computer on which the keylogger is installed.

E. Impersonation

It is possible to impersonate a program on a computer by launching windows that look like something else. For instance, let's say you login to the MSN® service and visit a website (in this case a hostile website.) It would be possible for this website to pop-up some windows that look like something else. They could look almost identical to windows that an inexperienced user might expect from his local computer. The user could be fooled into submitting information to the hostile website. For instance, consider the effect of seeing the following series of windows: If these could trick you into entering your password, then you could end-up sending your password to the attacker. Windows such as these could be created to mirror virtually any program or series of actions. Your browser will likely identify your operating system and your IP address might identify your ISP. Therefore, a hostile website could target you with a series of screen shots that look exactly as they should on your system. The key is that the screen shots are not coming from your system, but are coming from the hostile website. First, creating such a hostile website is probably fraudulent and illegal. We do not recommend or condone this activity. To protect yourself against this type of attack, make sure to configure your browser for high security and enable warnings for any code that is executed on your system.

F. Sniffing

If two people do not share the same computer, but do share the same network, it may be possible for one to sniff the others' packets as they sign-on. The traffic between your computer and the internet site you are accessing may be able to be recorded and decrypted or "played-back." This is not a simple attack to execute, but is possible if two people are close to one another and share a hub. Again, this is likely to be illegal and we do not condone this activity.

G. Social Engineering

Social engineering is the name given to the art of attacking the person, rather than the computer or system. The basic principle is that many people can be talked into giving someone else their id and password if they think it is someone that they can trust. For instance, I might call someone and say I was from AOL and that I was finally getting around to responding to their technical support question. I would then ask you to describe the problem that you are having and tell you that we have a solution. However, I just need to verify the account. Can you give me the username and password again? A surprising number of people would fall for this obvious scam. There is no limit as to how elaborate this can be. The more information that is given by the caller, the more realistic or believable the call is. Again, never give your password to anyone. No legitimate customer service representative will ask for this information. These are the basic methods that we are aware of for hacking an AOL®, Yahoo®, Hotmail® or any other dial-up or on-line password. Hopefully this will answer some questions and help you protect yourself against these attacks.

Figure.2 Basic needs for Hacking

learn about computers - in as much detail as you can- now most people will disagree with this but the first thing you should do is learn HTML this way you will know how to make decent websites. you may wonder why? because hacking is knowing everything about a computer an using that knowledge to get what you want. Now after you have done this you can start on this list of things to do.

Code

1. Learn about hardware - basically how your computer works.
2. Learn about different types of software.
3. Learn DOS.(learn everything possible)
4. Learn how to make a few batch files.
5. Port scanning. (download blues port scanner if it's your first time)
6. Learn a few programming languages HTML,C++,Python, Perl.... (i'd recommend learning html as your first lang)
7. How to secure yourself (proxy, hiding ip etc)
8. FTP
9. TCP/Ip , UDP , DHCP
10. Get your hands dirty with networking
11. Learn this assembler language (its the most basic language for understanding machine language and very useful to understand when anything is disassembled and decoded)
12. Learn to use a Unix OS. (a Unix system is generally loaded with networking tools as well as a few hacking tools)
13. Learn how to use Exploits and compile them. (Perl and C++ is must)

4. SHOP ADMIN HACKING

This method is use for testing the knowledge or for getting the credit card for shopping on internet or for fun or any way but not for cashing (because this method don't give PIN - 4 digit password) only give cc numb , cvv2 and other basic info.

Shopadmins are of different companies like : VP-ASP , X CART .. ETC. I am posting tutorial for hacking vp-asp shop. I hope u seen on internet whenever u try to buy something on internet with cc they show u a well programmed form very secure, they r carts .. like vp-asp xcarts . Specific sites are not hacked but carts are hack.. below i m posting tutorial to hack VP ASP cart. now every site which use that cart can be hacked and through their *mdb file u can get their clients ' credit card details ' and also login name and password of their admin area. and all other info of clients and company secrets.

A. Here We Go

Type: VP-ASP Shopping Cart Version: 5.00How to find VP-ASP 5.00 sites hmmm, Good Q. Finding VP-ASP 5.00 sites is so simple...Go to google.com and type .in title: VP-ASP Shopping Cart 5.00You will find many websites with VP-ASP 5.00 cart software installed Now let's go to the exploit..the page will be like this >****://***.victim.com/shop/shopdisplaycategories.asp The exploit is: diag_dbtest.asp so do this>****://***.victim.com/shop/diag_dbtest.asp A page will appear contain those: xDatabaseshopping140xDblocationresxxdatabasetypexEmail xEmailNamexEmailSubjectxEmailSystemxEmailTypexOrder number.:. EXAMPLE...The most important thing here is xDatabase: shopping140ok now the URL will be like this:****://***.victim.com/shop/shopping140.mdb if you didn't download the Database..Try this while there is DB location. xDB location resx the url will be:****://***.victim.com/shop/resx/shopping140.mdb If u see the error message you have to try this :****://***.victim.com/shop/shopping500.mdb download the mdb file and you should be able to open it with any mdb file viewer, you should be able to find one atdownload.com Or use MS Office Access. inside you should be able to find credit card information. and you should even be able to find the admin username and password for the website. the admin login page is usually located here****://***.victim.com/shop/shopadmin.asp if you cannot find the admin username and password in the mdb file or you can but it is incorrect, or you cannot find the mdb file at all then try to find the admin login page and enter the default passwords which are Username: admin password: admin or username: vpasp password: vpasp

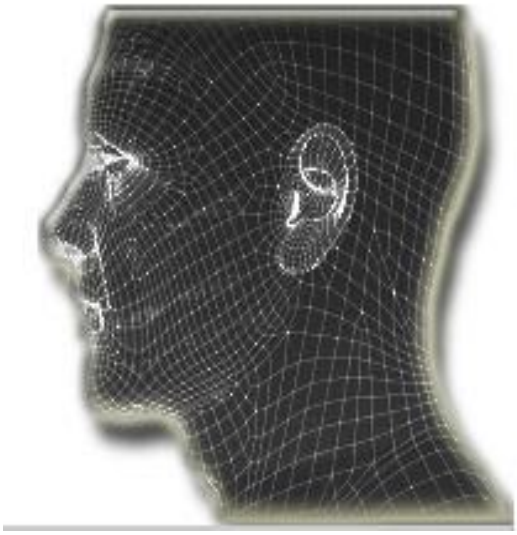
5. HACKING WINDOWS XP

- Boot the PC in Safe Mode by pressing the F8 key.
- Select the Safe Mode option, now you can now Login as an Administrator and XP won't prompt for the Password.
- Try rebooting the PC in DOS.* Now, Access to C:\Windows\system32\config\SAM.
- Rename SAM as SAM.mj.
- Now XP won't ask for Password next time you Login.
- Now, again go to Start menu --> Run.
- Type there cmd prompt.
- Type net user *, It will list all the users.
- Again type net user "administrator" or the name of the administrator "name" *.
- It will ask for the password. Type the password and there you are done.
- Hold the Ctrl+Alt key and press Del twice. This will bring up the normal login and you can log on as Administrator. To unhide the Administrator account so it does show up.
- Again go to Start --> Run --> regedit.
- Go to HKEY_LOCAL_MACHINE --> SOFTWARE --> Microsoft --> Windows NT -->

Current Version --> Win logon --> Special Accounts --> User List.

SOURCE:

WWW.OUG-ARENA.COM(ORKUT UNDER GROUND)



Book: The Secret of Hacking – Mr. Manish Kumar
Publications – Chief Security Officer – Leo Impact Security

6. CONCLUSIONS

It is for educational purpose only .Try to secure your pc from the hackers. Do not think hacking is crime.Hacking is not a crime depends upon user the user mind set will be change. In this generation every process along with computer we need to know whether our data is secure or not