2012

Shield Against Hacking

Praneet Menezes

1/11/2012

CREATE EBOOKS IN 30 SECONDS WITHOUT WRITING A WORD

CLICK HERE TO SEE HOW

Copyright notice

ISBN -> 978-1-300-34435-3

Liability disclaimer

The words “hack” and “hacking” as used in this book imply “ethical hack” and “ethical hacking”.

The author of this book does not dispense advice on hacking or prescribe the use of any technique for hacking. The intent of the author is only to offer educational information to help the reader develop a hacker defense attitude to prevent the hacking attacks discussed.

In the event a reader uses any of the information in this book for the purpose of unlawful hacking and causing damage, directly or indirectly, to anyone, the author disclaims all liability and assumes no responsibility for their action.

Foreword

Hi there, folks!

I am Praneet Menezes, 17, studying in FY, and the book you are reading is the first book I have ever written. Noticing how ignorant most people are about cyber security, I decided to write *Shield Against Hacking* to educate them about the hazards of hacking and what they could do to safeguard themselves from the attacks of hackers.

I have gathered the anti-hacking information you are about to read from various authentic sources and presented here in simple language and easy format. I am sure you will enjoy the book and use it to your benefit.

Dedication

To my mom and dad

Special Thanks

To Mr. Crizan Menezes, Mr. Prakash Deshmukh & Mr. Sebastian Gonsalves

CONTENTS

Chapter 1: Introduction
How to use the book?
Who is a hacker ?
Types of hackers

Chapter 2: Online accounts
Phishing
Primary email address
Social engineering
Guessing passwords
Shoulder sniffing
Dictionary attack
Security questions
Brute-Force attack
Hacking using mobile phones
Hacking using firesheep
Pharming or DNS spoofing

Chapter 3: Wireless networks
Type of encryptions
Use of packet sniffers

Chapter 4: Hacking using viruses
Types of malware
Keylogger
RAT's
USB viruses

Chapter 5: Miscellaneous
Windows administrator password
IP hacking
Burn note
Browsers

Vote of thanks
Reference
Contact info

Introduction

In the modern world of today, where everything from shopping to banking is available on the web, even the cyber frauds and hacking accounts have become increasingly sophisticated. A hacker can use a computer program of a very small size to find your password, steal your data, and rob you of every penny in your bank account. And, oops! Who do you think is caught up in the legal hassles following a cyber crime? Although you could go to the cyber crime cell of the police, it is always the victim who 'faces' the law, rarely the hacker himself.

As prevention is always better than cure, read this book and prevent your accounts from being hacked.

How to use this book ?

In this book, you will find out how hackers hack a computer system or an online account. You will also find out how one may safeguard oneself from hacking. THIS BOOK TEACHES WAYS OF PROTECTING FROM HACKERS, NOT WAYS OF HACKING.

This book is a must read for IT and other professionals, cyber security officers, businesspeople, bureaucrats, organizations handling sensitive information, government bodies, in fact, anyone who wants to secure themselves against cyber crimes.

Who is a hacker?

A hacker is a computer pro who is very well acquainted with computers. They like to explore and learn how computer systems work, finding ways to make them do what they do better, or do things they weren't intended to do.

There are two kinds of hackers: white hat and black hat.

White Hat: They are the good guys. They don't use their skills for unlawful purposes. They usually become Computer Security experts and help protect people from Black Hats.

Black Hat: They are the bad guys. They usually use their skills maliciously for personal gain. They are the ones who hack banks, steal credit cards, and deface websites.

Types of hackers

Beginners: They are the wannabe hackers. They are looked down upon in the hacker community because they make hackers look bad. They often do not have hacking skills and use tools developed by other hackers without knowing what is happening behind the scenes.

Intermediate hackers: They know about computers and networks, and have enough programming knowledge to understand what a script might do. However, like the beginners, they use pre-developed well-known hack tools to carry out attacks

Elite Hackers: They are skilled hackers. They are the ones who write many hacker tools and exploits out there. They can break into systems and hide their tracks or make it look like someone else did it.

Online Accounts

Online accounts mean email websites, social networking websites such as Gmail, facebook etc and any other account that you might be operating from the internet. In this chapter I will discuss various ways in which online accounts can be hacked as well as their countermeasures. There is no such thing as facebook hacking software or Gmail hacking software. People think that entering user name in hacking software would automatically hack the password for you. It is a myth. And if you find any such software on the web then they are Trojans or viruses. I will discuss viruses later in the book.

Here are the ways for hacking online account:

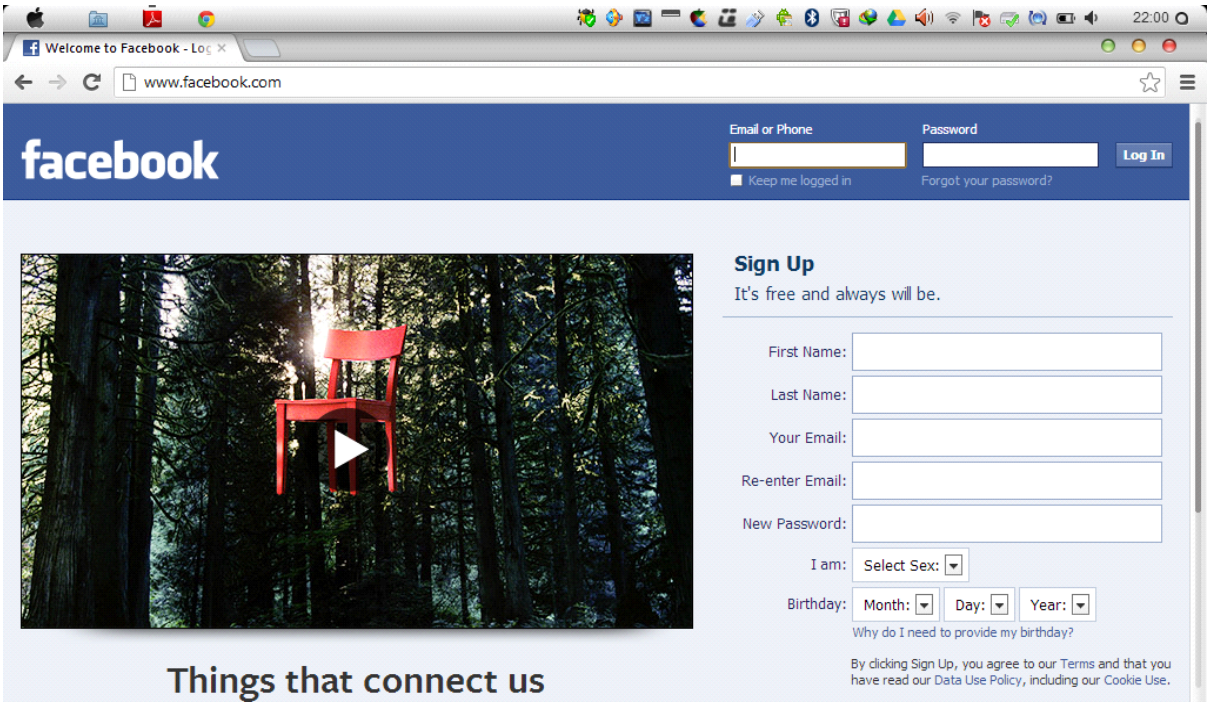
1. Phishing

Phishing refers to a process in which a hacker pretends to be someone he is not. In phishing, a victim receives a fake page which is the exact replica of an original page. This fake page is stored on a file hosting a website and a link to this page is sent to the victim via email. As soon as the victim opens the link, the fake phishing page opens. Then as soon as the victim enters his details, his sensitive information such as user name and password gets stolen.

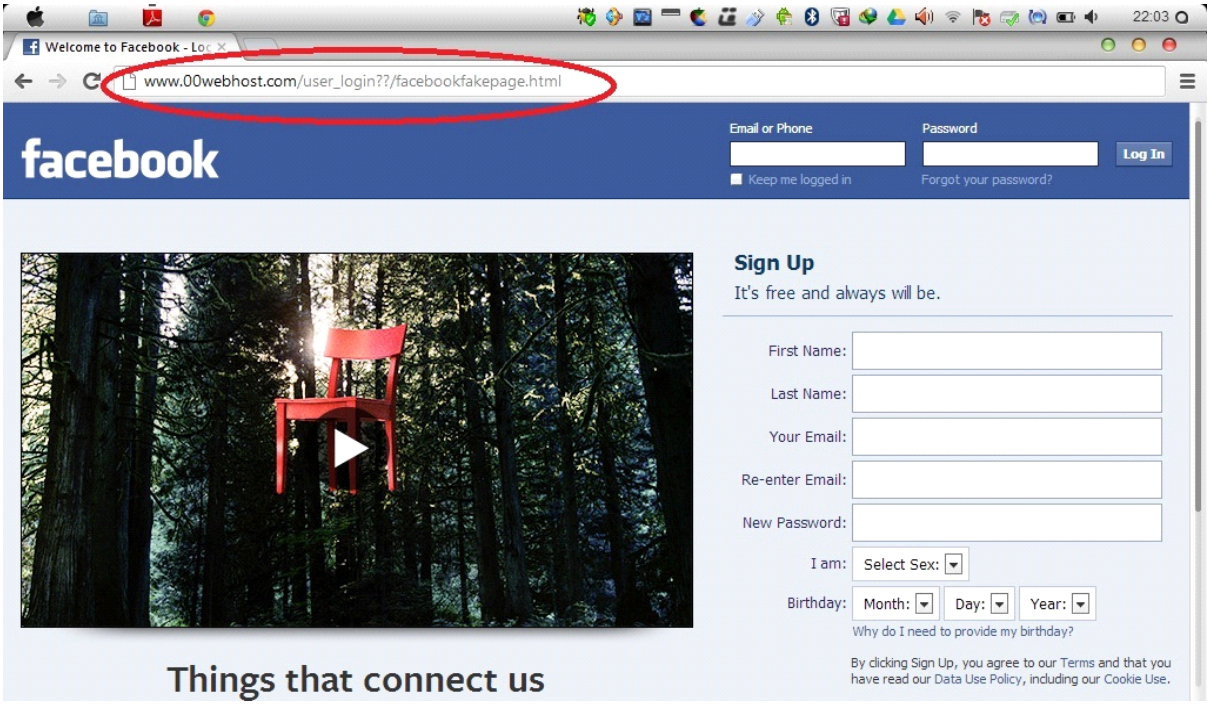
The hacker then redirects the victim automatically to the real facebook page. The victim thinks that they must have entered a wrong password and so they enter it again on the real facebook page. This time they get logged on to facebook, and so do not know they were a target of phishing. Now knowing the user name

and password, the hacker can login into the victim's account and cause trouble for him.

Here is an original facebook page :



And here is a replica of the facebook page used in phishing :



Countermeasure:

As you can see, the only difference between the original and fake pages is their URL. The URL for original facebook page is www.facebook.com whereas it is different for the fake page. Hence the difference in URL is the tool for identifying if the website is real or a phishing attack !

Website developers and software engineers are well aware of phishing. Hence modern web browsers come with anti-phishing technique. Example of such a browser is Chrome browser by Google Inc

To activate anti-phishing measures, you must go to settings in the Chrome browser, then click ‘show advanced options’ and then check the anti-phishing box in ‘privacy tab’.

2. Primary email address

Social networking websites use email for recovery of passwords. When recovery of password is selected in facebook, an email is sent to your email address which consists of your username and password. If a hacker gets access to your email id, it will be very easy for them to hack your account and various other accounts that are linked to email address.

Countermeasure:

Never let anyone have information about your primary email address. Remember that your email id is more important than your facebook. If your facebook is hacked, only your facebook account is hacked but if your email id is hacked then there is a threat that all other online accounts linked to the email address will be hacked too. So protection of your email id is of utmost importance.

3. Social Engineering

It is an old-fashioned way of obtaining a password from someone by pretending to be their well-wisher. For example, a hacker may call posing as a bank employee and tell a victim that there are upgrades to their credit card. He may ask the victim to reveal their credit card number as they have received some bonus points for the credit card. Likewise he might also ask them for passwords and other sensitive information with which he could hack the victim's bank account. And in their greed for some extra bonus points, the victim would readily reveal their bank information and – BAM! – All the sensitive information is lost in less time than it takes to blink. Often people tell their online account passwords to their trusted friends and then their accounts get hacked.

Countermeasure:

Never reveal your personal information to anyone. Moreover never trust anyone who claims to be your well-wisher. In most of the hacking cases, the hacker is a trusted friend of the victim, knows the victim's personal data and uses this information to hack the victims account. When it comes to bank account details or online account passwords, the only person you can trust is none other than yourself.

4. Guessing Passwords

Guessing passwords is a common way of hacking. Usually people form their passwords from their names, names of friends, lovers, girlfriends and boyfriends or their phone numbers, dates of birth and such things. Guessing passwords is surely the easiest way of hacking.

Countermeasure:

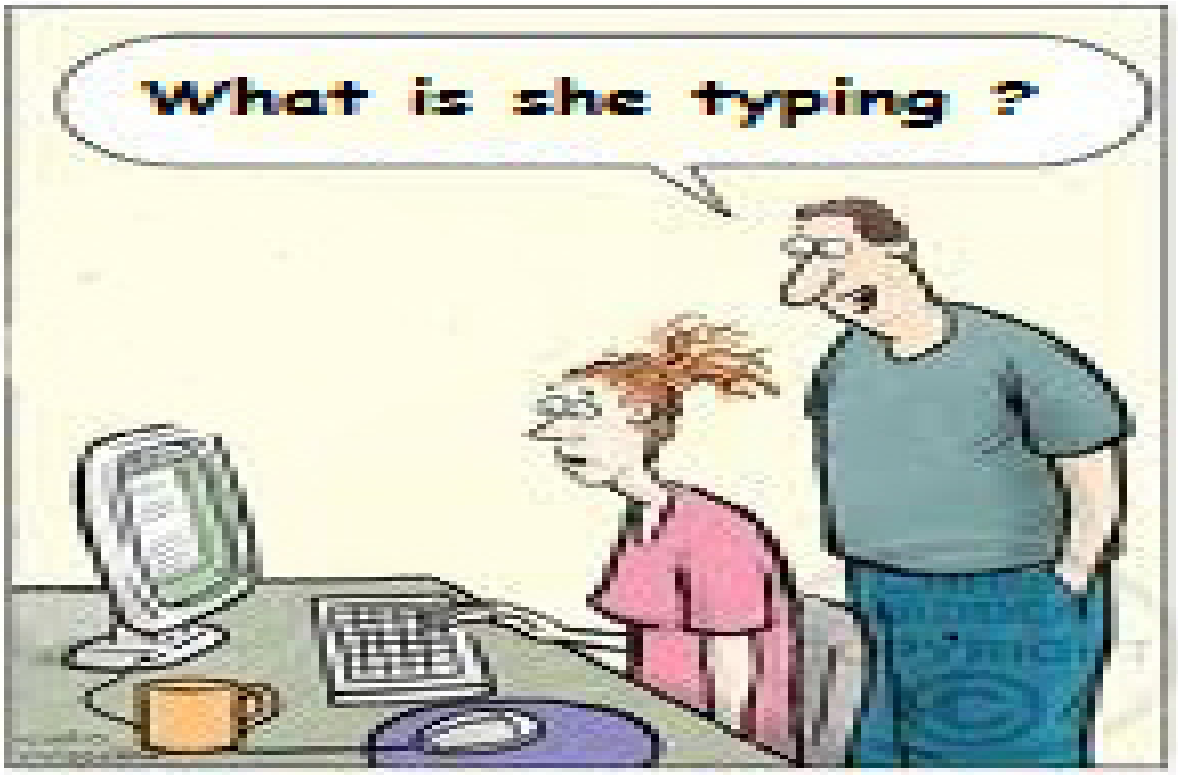
The only countermeasure is to never use a password that is easy to guess. Keeping difficult to crack yet easily remembered password is certainly a good thing. For example, a password like "hello2U" is easy to remember yet difficult to crack. Similarly, we can use a combination of numbers and symbols with lowercase and uppercase alphabet.

5. Shoulder Sniffing

Shoulder sniffing is exactly what it says – a hacker simply attempts to look over your shoulder as you type in your password. The hacker may also watch whether you look around your desk for a written down reminder or the password itself.

Countermeasure:

When you type in your password make sure there is no one behind you attempting to peak. Make sure you don't keep any sticky notes lying.

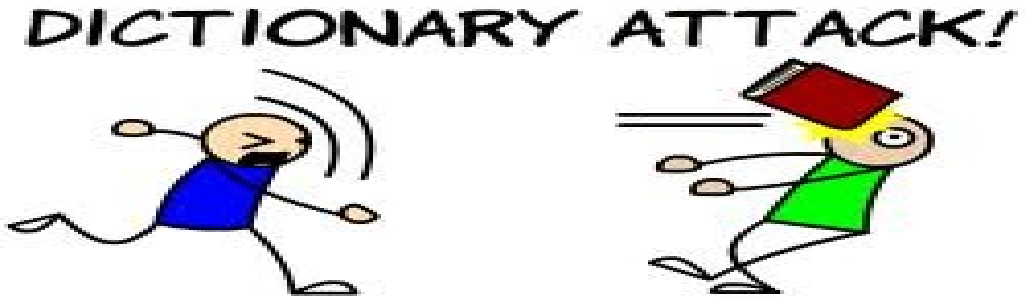


6. Dictionary Attack

In dictionary attack, a hacker tries all common passwords and all words in a dictionary as a password. There are high tech software's which automatically try all worlds in the dictionary to crack a password. But this is not a very effective way of cracking passwords.

Countermeasure:

The only countermeasure is not to use passwords that are listed in a dictionary. Also make it a point to change the default passwords such as 12345 or 0000 which are preset in mobile phones and internet provider's dial-up connections.



7. Security Questions

Several websites offer password recovery options such as answering security questions to change passwords. If a hacker is someone you trust then he could answer your security questions and hack your account. Moreover, security questions which are answered by your mother's name, your first grade teacher's

name, street address, favorite movie title or pet name are easily guessed by the hacker.

Countermeasure:

Never reveal personal data to anyone. Besides choose security questions that are difficult to guess.

Security questions could be changed too. Here is how to do it on yahoo. Once you have logged on to yahoo, click on your name at the top left corner, then click on 'account info', and then on 'update password-reset info'. Next select the 'change security questions' button. I advise you to create your own security questions. Give alternate email id and phone number at the websites. Hence even when your account gets hacked, you could recover it.

8. Brute-Force Attack

This is a way of password cracking in which permutation and combination are used. The software tries all possible password combinations. The software takes minimum and maximum number of digits a password could have. It also asks for the type of password such as alphabetical, numerical, alphanumerical or symbolical. From these inputs the software generates all possible combinations which at times could run into to millions and billions. The software tries out password combinations at a rate of 3500/sec. Thus, given enough time, the password is cracked. Brutus AET2 is one such software.

Countermeasure:

Brute-force attacks may be prevented by creating a very long password using many numbers and characters. The longer the

password the harder it gets for the hacker to crack your password. If the hacker fails to crack your password even after trying for a few days then he is very likely to just give up.

Software developers now offer a new countermeasure that allows a password to be tried only thrice after which the account is temporarily locked.

9. Hacking Using a Phone

A hacker uses a victim's mobile phone as a tool for gaining access to their account. Spy software's available for mobile phones do this easily as there is very low awareness of mobile viruses. Very few people install anti-virus on their mobile phones. So the hacker takes your phone and installs the spy software. The installed software is hidden and cannot be viewed by anyone except the hacker.

Countermeasure:

Never install any software from unknown sources into your phone. Always install anti-virus in your mobile phone. Never allow anyone to install anything into your phone.

10. Hacking Using Firesheep

Firesheep is a plug-in developed for Mozilla Firefox browser. The plug-in uses the method of packet sniffing for hacking the accounts. It captures unencrypted cookies from websites. However, a drawback of Firesheep is that the victim's computer needs to be in WLAN or LAN of the hacker's computer for capturing cookies and it works only when the user has signed into their online account.

Countermeasure:

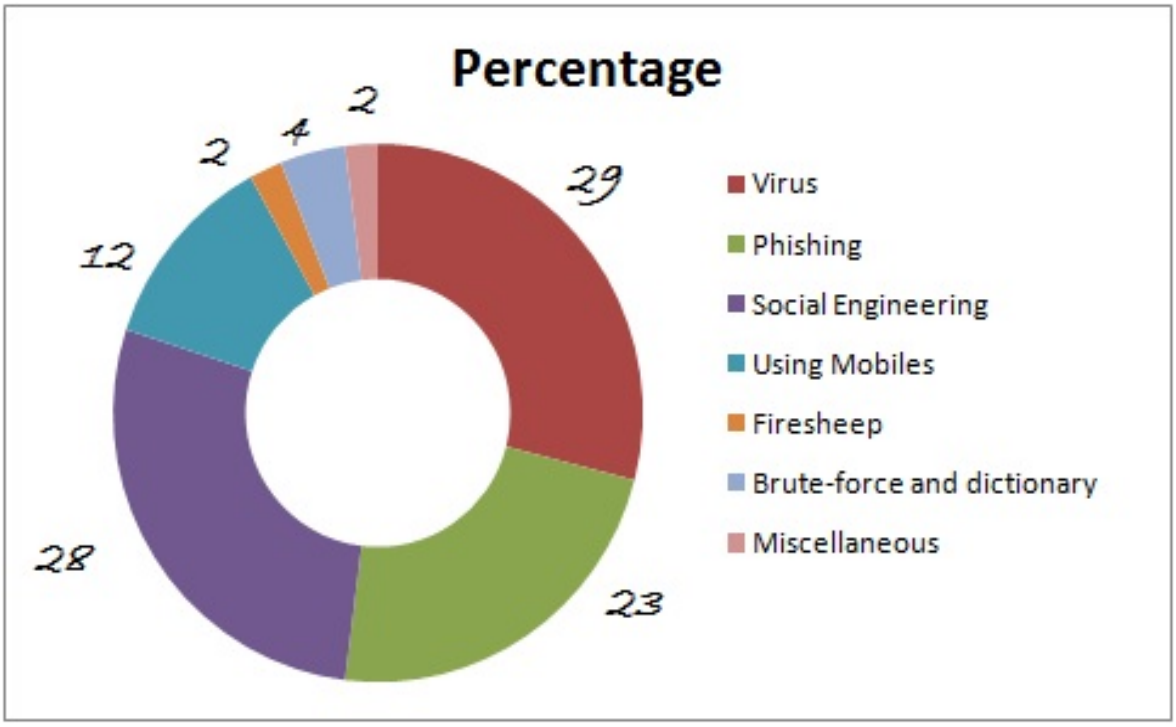
Firesheep is an old method and various remedies are already out. Firefox browser after v3.5 does not support Firesheep and another plug-in called Blacksheep was developed to stop the attack of Firesheep.

11. Pharming or DNS Spoofing

We have seen how phishing attack works and how it can be identified using URL. But what if the URL is correct and the page is still a phishing page ? Confused ? Well this can be done using pharming. The hacker gets into your IP address and then makes changes in the DNS and IP address. So even if you enter the correct website name, it will still take you to the phishing page and allow your password to be stolen.

Countermeasure:

Do not reveal IP address to anybody. Always look for secure logging websites. Websites with https:// are always secure and cannot be used for phishing or pharming attacks. Always look for the https:// before logging into a website where you have to enter your details such as user id and password. Gmail is an example of website with the https:// mark. Thus pharming can be prevented.



The Pie diagram shows the percentage distribution of hacking attempts.

Wireless Network

Nowadays there are wireless hotspots everywhere! You can get internet access with a wireless-enabled laptop almost anywhere you go. In this chapter I will discuss ways a hacker goes about getting into secure wireless networks and what he does once he is inside.

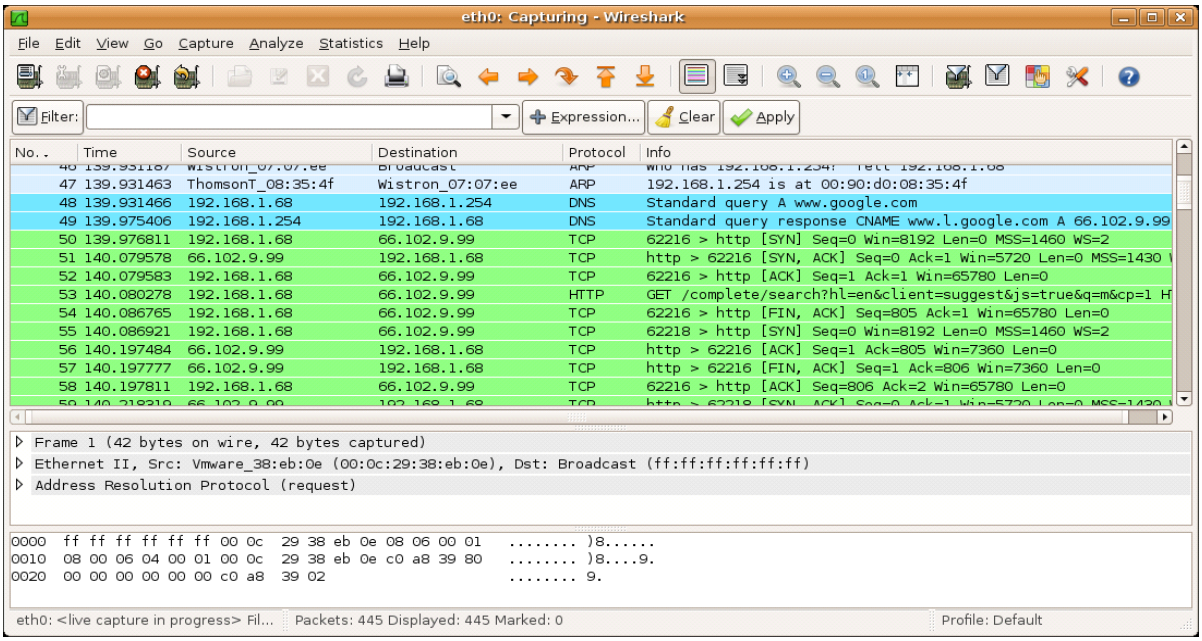
There are basically two security encryptions for wireless networks: WEP and WAP.

WEP (Wired Equivalent Privacy): WEP is not considered safe anymore. It has several flaws that allow a hacker to crack a WEP key easily.

WAP (Wireless Application Protocol): WAP is currently the most secure and best option to secure your wireless network. It is not as easily cracked as WEP because the only way to retrieve a WAP key is to use a brute-force or dictionary attack. If your key is secure enough, a dictionary attack won't work and it could take decades to crack it if you brute-force it.

12. Use of packet sniffers

WEP is cracked using a Linux distribution called backtrack which uses numerous software's necessary in cracking WEP encryption. The basic idea behind cracking WEP is to capture the packets that are being sent from a wireless router. Each packet is about the size of 3 byte. The WEP encryption is broken when 30,000 bytes are captured. After cracking, the hacker gains access to your passwords, IMs etc. Wireshark and DSniff are two of such packet sniffers



Here is a screenshot of Wireshark capturing packets of data.

Countermeasure:

1. Change your routers default password and make sure you have WAP encryption enabled. If your router doesn't have a WAP option, use WEP. It is better than nothing.
2. Use a long secure password for your router. Include numbers, lowercase letters, uppercase letters and other symbols. The more complex your password is, the better the chances of it not getting hacked.
3. Make sure your router has the option to not broadcast your SSID enabled. This will prevent some programs from locating your wireless network.
4. Every wireless card and wireless adapter has a MAC address. By choosing to allow only your MAC addresses onto the network, you can keep a lot of attackers out.
5. Make sure to use SSL (Secure Socket Layer) encryption for the important sites like banks. You can tell if the site has SSL enabled when the URL begins with https:// instead of http://.

6. In cafes or other hotspots where internet is free, packet sniffing is very common. To avoid being affected use a VPN (Virtual Private Network) service to encrypt the data you send across the internet

Free VPNs can be downloaded for use. ProXPN VPN is free and can be downloaded from the link below:

Download ProXPN VPN

Hacking Using Viruses

Malware is a big problem today. Everyday thousands of innocent people are getting infected by different types of malware. The most common types of malware today are viruses, worms and Trojans. In this chapter I will discuss all the types of malware and viruses.

Let us begin with knowing who is who:

Viruses: Viruses cannot spread without the help of us humans. They are like parasites because they need a host to attach to. The host is usually a legitimate looking program or file. Once this program is launched, the virus is executed and infects other files on your computer. Viruses can be very destructive. They can damage your computer hardware, software and files. Viruses are spread through the sharing of files and are often sent with emails via attachments.

Worms: A worm is a malicious program that can replicate itself onto other computers on a network. Unlike viruses, worms don't need a human to be able to spread and infect systems. Once it infects a system, it uses that system to send out other copies of itself to other random systems attempting to infect them.

Trojan Horse: A Trojan horse is a malicious program that can be used to do silly things to a system like changing its desktop, mess with the user interface, and take control of your mouse. It can also be used for some serious things like accessing your data, erasing your files, stealing your passwords, and capturing your keystrokes.

Bacteria: Bacteria make many copies of themselves and eventually end up taking up all of the computers resources such as all of its processor power, memory and disk space. This results in the user losing resources

Blended Threats: Blended threats combine all of the characteristics of the above and use them along with the system vulnerabilities to spread and infect machines.

13. Keylogger

Keylogger is software that records the strokes of the keyboard. Every letter you type on the keyboard is stored in the keylogger program. Some hi-tech keylogger's can also record web history, take screenshots as well as web cam shots. They can also record your passwords and private chat history from gtalk or facebook. These stored logs are then sent to an email or FTP address as soon as the infected computer is connected to the internet. Thus the hacker can monitor your actions, get your user names and passwords and a lot of other sensitive data just sitting at home. However keylogger is passive tool that does not harm your computer or corrupt any files. It only monitors your computer. Winspy keylogger is a well-known keylogger.

14. RAT (Remote Administrative Tool)

RAT is similar to keylogger. In fact, keylogger is a part of RAT– the most dangerous of all viruses! Like keylogger, RAT records all activities of the computer where it is installed. But RAT is not passive. A hacker can use it to damage your computer by deleting files and installing malicious virus on your computer remotely sitting far away at home. The hacker can shut down or restart your PC. He can also freeze your mouse and keyboard. Also, files on your computer are visible to the hacker and hence important data can be stolen or deleted easily. ProRAT is one such deadly RAT.

Countermeasure:

But thank God for anti-viruses which can easily detect a keylogger or a RAT and quarantine it before it is installed on your PC. But hackers too are very smart. They attach the virus to any other file such as text, video or another program. This is done using binders and crypters.

Crypter is software that makes some minor changes in the codes of the virus so that it goes undetected by anti-viruses.

Binder is software that binds two software's to form one .exe

A hacker may attach the malware to a useful application, such as a game, and give it to the victim. The hacker may also tell you to disable anti-virus making some reason such as 'the program is cracked so please disable your anti-virus' etc. But the hacker may also attach a virus along with the program. Thus your computer is infected. And anti-virus would find it difficult to remove the virus once it is installed. It is very difficult to differentiate normal software from virus-infected software as viruses have a very small size, say 300KB, whereas software's may be of size 500000KB

Take these steps to safeguard from the attack of viruses:

1. Make sure you have good and up-to-date anti-virus software installed on your computer. Also if there is an automatic update option on your anti-virus software, make sure it is enabled.

2. Make sure you have a firewall installed on your computer and see to it that it is actually enabled. Firewalls protect against unauthorized incoming and outgoing connections.

3. Never install any software that is from unknown sources. If you want to install VLC media player, then make sure you download it from its official website www.videolan.org

4. Free software's over the internet may look good but may also have a good amount of viruses ready to attack your system.

15. USB viruses

USB viruses run automatically into your computer as soon as a USB pendrive is inserted in your computer. Within seconds all the data such as passwords and user names stored in your browser is stolen and saved in a file in the pendrive. And you don't even know that your data is stolen. There are all types of malwares that spread through USB drives. Nowadays there are various micro size pendrive's and USB drives hidden in various forms such as hand band and necklaces. They have now become likes explosives that can be sniffed and plugged into computers. So we need to be extra careful about pendrive's.

Countermeasure:

Never plug in any pendrive, thumbdrive and memory sticks from unknown sources into your computer. Even when the USB is from a known source, make sure that it is virus free by using anti-virus before you explore the pendrive.

In this book using anti-virus is emphasized much. You need not buy expensive anti-virus and upgrades. Several free anti-viruses also act equally well. Avast is one such free anti-virus. You can download and install it free. Click the link here to download Avast.

Avast Download

Miscellaneous Hacks

16. Windows Administrator Password

Windows administrator password is very important in securing your computer. You can secure your online accounts and wireless networks but if you fail to protect your main windows PC, the rest of securing is useless as a hacker could still use your PC to access your data.

Windows administrator password is stored in a file called SAM in the windows components. A hacker gets physical access to your PC and then uses an operating system stored in a pen drive or optical disk. Linux is one such operating system that can be accessed from an external hard drive. This is done by going to BIOS (Basic Input Output System) settings, changing the boot disk to external hard drive or optical disk, and booting the operating system. Then the hacker finds the SAM file, brute-forces it and cracks the administrator password.

Countermeasure:

Do not let unknown people access your computer. Importantly, we must always set a password for the BIOS. This can be done by pressing F2 before windows boots. This should be done as soon as the computer is switched on. Press F2 amd watch a blue screen appear. Use the right arrow key and go to the security tab. Then select the last option i.e. Password on Boot. Enable it and set a password.

17. IP Hacking

IP stands for internet protocol. It is a unique number given to a computer so that it is differentiated from all other computers.

NetBIOS stands for Network Basic Input Output System. It allows LAN or WAN to share drives, folders, files and printers.

Gaining access to a computer through NetBIOS is very simple. The only thing required for the target machine is to have file and printer sharing enabled and have port 139 open. A hacker first scans for any active IP addresses and then looks for any shared resources such as a drive or a printer. The hacker then pings to this IP via cmd and gets access to your files on shared files.

Countermeasure:

To avoid NetBIOS attacks, just disable file and printer sharing. It is disabled in Windows Vista by default but you must do a little work in Windows XP. Click on the start button and go to the control panel. Select network connection. If network connection is not available then try changing view from top right corner. Select your active connection. In my case it is Wireless Network Connection 1. When a window opens, click on properties button. Deselect ‘File and Printer Sharing ‘and click on ok.

18. Burn Note

I strictly recommend not revealing your passwords to anybody anytime, yet there may be many situations where you are required to reveal your password to someone. The person, whom you are giving your password, may be a trusted person and they may not give it to anybody, but what if his account is hacked? Then the hacker gets to know your password as well. This comes as a bonus to the hacker as he gets two passwords in one go.

Countermeasure:

There is a solution. We can create self-destructive messages. This message operates on a timer. The message you sent gets automatically deleted when the time is up. There are free websites which help you create self destructive messages. One of them is www.burnnote.com

You can create notes using this website. You get a link to this note. Now send this note to the person whom you want to reveal your password. As soon as the recipient clicks on the link, the message opens and they get your message. As soon as the timer comes to zero, the message is destructed and the link you sent is no more valid. Thus your data remains confidential and is not exposed. Other sensitive information can also be sent using this facility.

19. Browsers

Browsers are an important part of the internet. It is not possible to access the internet without the browsers. It is possible to hack through browser features. For example, many browsers offer to store passwords and user names so that you don't have to put your passwords again and again. This makes logging into websites easy but it makes hacking easy too. Stored passwords can be retrieved easily. If a hacker gets physical access to your computer then he can get all your passwords. History is another feature that the hacker can access. History can be used to know what is person has been doing online and keep a track of his activities and whereabouts.

Countermeasure:

Browsers also have many other fantastic features which we can use to save ourselves from the hackers. Once a download is finished the browser scans the file for viruses and then only lets you install it. Some browsers have anti-phishing techniques.

Browsers also have another feature called 'Private Browsing'. In this feature we can hide history. After private browsing is turned on there is no record of the history. Thus it is not necessary to delete the history again and again. Browsers like Safari by Apple Inc and Mozilla Firefox offer private browsing. Its free and easy to set up ! Click below to download Apple Safari browser And Mozilla Firefox

Download Safari Download Firefox

Epilogue

Thank you for having read the book. Now you know a great deal about hacking and shields against hacking. I am sure you will use the book for yourself. I hope you will tell your friends about this book so they too could use it for themselves. What more does an author want? Thanks and cheers and lots of looking forward.

Keep in touch

I would love to hear what you have to say about the book.

So please email me your comments.

Or come to my facebook page *Shield Against Hackers.*

Or ask me for personal and corporate sessions.

Phone > +918551889227

Email > praneet.menezes@ymail.com

Website >www.shieldagainsthacking.com

Visit Shield Against Hackers website now !!

Reference

- www.google.com
- www.wikipedia.com
- Hacking for dummies
- McGraw Hill Wi-Fi security
- Hacker’s Underground Handbook

Back Cover

Are you really safe online?

A hacker could access your social networking website and cause irreparable damage to your image.

Or even worse, they could hack your bank account and leave you bankrupt.

Who could help if this happens to you? Cops? No, friends, the first and the only person who could help you are yourself. The best way is to take precautions and prevent hacking.

This book tells you about two things:
> How hackers hack
> How you could stop them

CREATE EBOOKS IN 30 SECONDS WITHOUT WRITING A WORD

CLICK HERE TO SEE HOW