# THINGS YOU DON'T KNOW
# &
# WHAT TO BE AWARE OF...

InfoSecurityLab

- Part 1. *What does "hacker" mean?*
- Part 2. *The hackers & the network*
- Part 3. *Hacker's profile*
- Part 4. *Possible dangers*
- Part 5. *Hackers' methodology*
- Part 6. *Latest methods of hacking*
- Part 7. *Script Kids*
- Part 8. *How to protect*
- Part 9. *We can beat them*

# Part 1

***What does hacker mean?***

# Term "hacker"

***There are a bunch of definitions of this term.***

***Some of them are the following...***

1. A hacker is a person with an intense love of computers, and because of this love he/she tends to have a deep curiosity about them.

InfoSecurityLab

2. A hacker is someone who likes to create or modify computer software and hardware. He/she is occupied with programming, administration and security related items.

InfoSecurityLab

3. Hackers have technical adaptness and a delight in solving problems and overcoming limits.

# Part 2

## ***The hackers & the network***

InfoSecurityLab

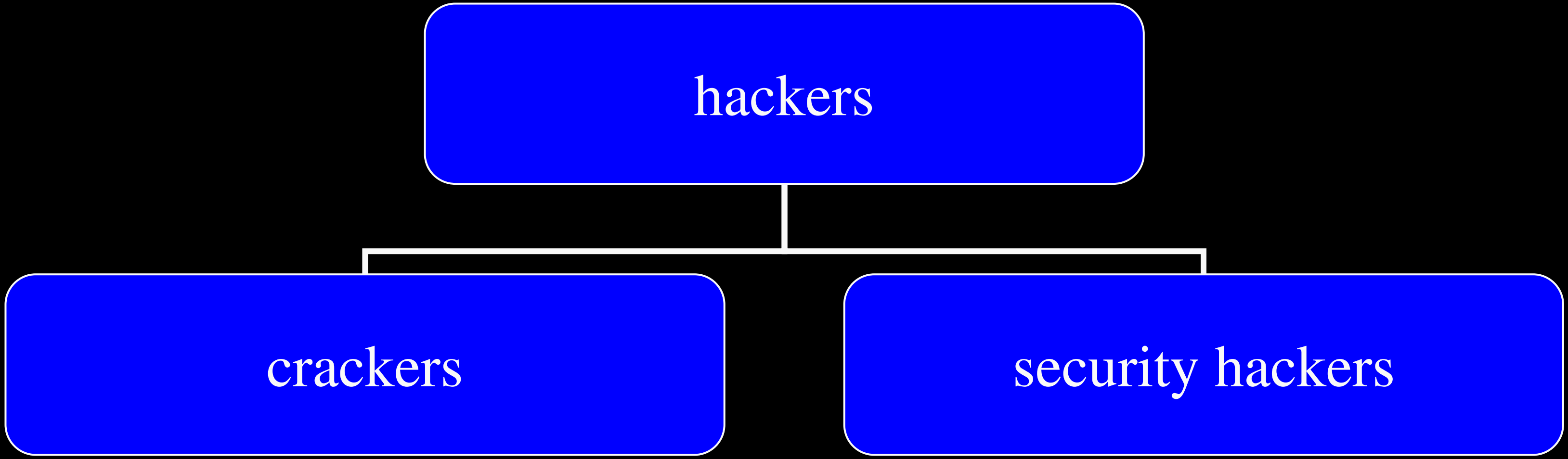
# World Wide Web

The internet was built for government and military researchers, to make their communication and information sharing easy. This is why it's designed to be open.

InfoSecurityLab

# World Wide Web

"*Hackers*" are the ones who built the internet and made it work. Some of them evolved through time and became what we call today crackers. The others ended up being involved with guaranteed security, trying to fight crackers.



InfoSecurityLab

# Internet World-Free World

## ***While the internet has defined a new area of communication, new definitions of searching through the internet have come to light.***

- Searching data of other people, started as an expression of human curiosity and ended up to be the worst nightmare for all of us.

- Our privacy is in danger and we have to protect ourselves with just being *aware*.

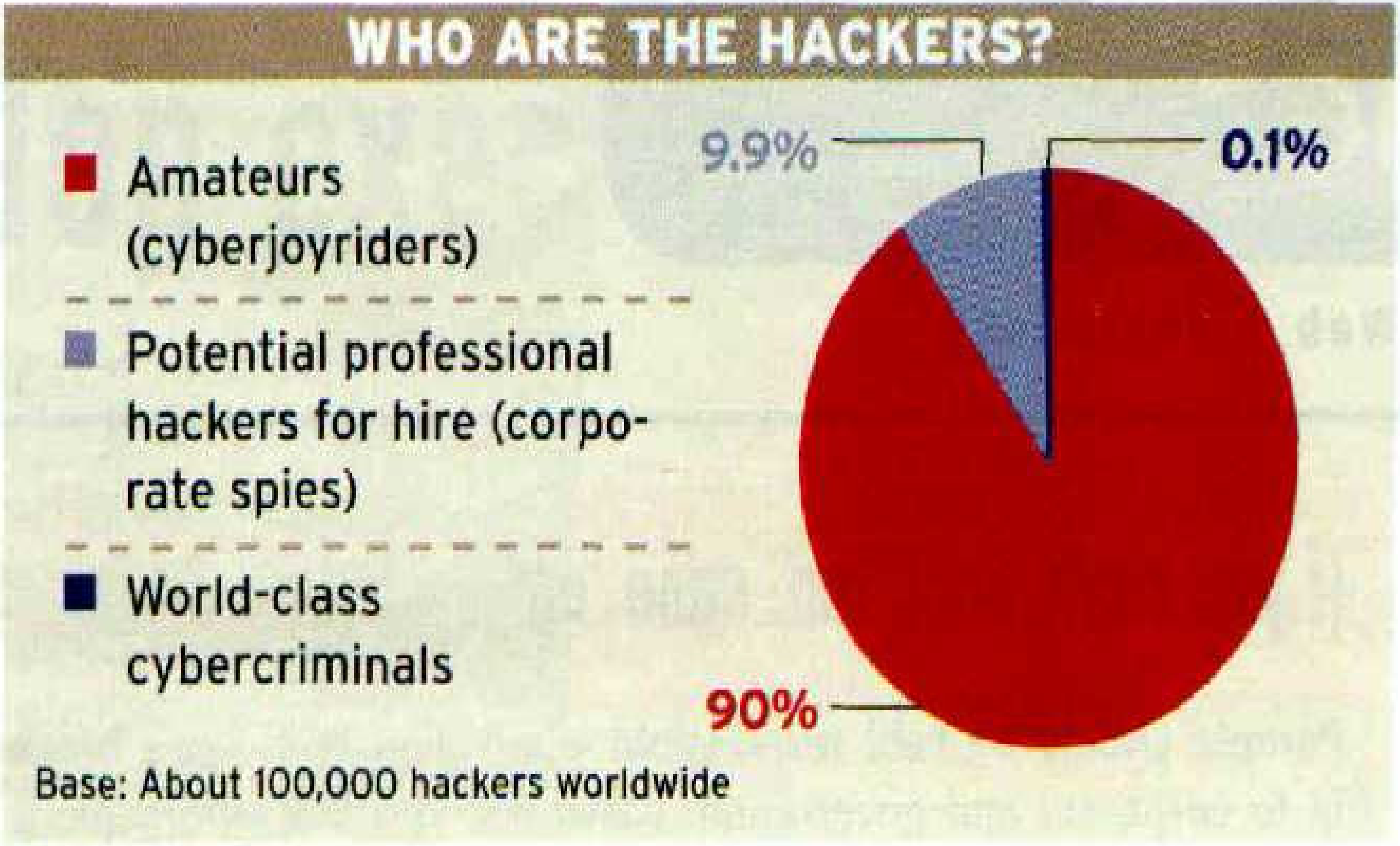
# Some true records...

*"I am old enough that when I studied computer science in college, the term hacker was used differently than it is today. At that time, hacker was a term used to describe someone who was enjoying coding too much, who liked to pick apart and explore how computer systems and software worked, beyond what was required in the professor's assignment. There was no malicious connotation to the term hacker at that time.*

*Indeed, those who travel the Internet with an exotic "nom de guerre" and like to explore the failings of computer systems have sought to reclaim the term "hacker" as the moniker of the good guy and seek to substitute the eponym "cracker" to describe the evil doers of computer sabotage. "*

**Jim Reavis**

**Network World on Security, 11/01/99**



Source: IBM Global Security Analysis Lab, Yorktown Heights, N.Y.

csciwww.etsu.edu/gotterbarn/stdntppr/stats.htm

# Part 3

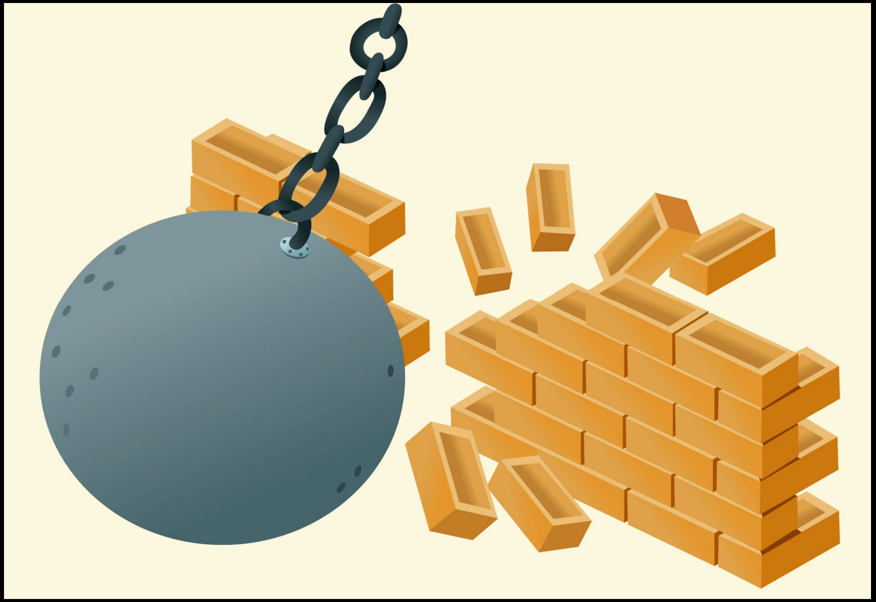
## ***Hacker's profile***

# Hackers-Crackers

***Hackers*** built the internet...

# ...but...

***...crackers*** **break it down.**



# On one hand...

- Hackers are considered as problem solvers and they believe in freedom and mutual help.
- Good hackers want to deal with interesting projects and they insist on control, so when something is broken they tend to fix it.
- They like to work for people with high standards and they fight criminal activity.

# Controversial...

- The other group of crackers-who insolently call themselves hackers-consists mainly of adolescent males trying to enter secure web-sites to wring private information out of them.
- They are considered to be lazy, irresponsible and not very bright persons, by their "colleagues" hackers.
- They like to create CHAOS.

InfoSecurityLab

# Crackers- their psychological profile

***Is bad hacking a disease? Is it possible to be addicted to it?***

# Characteristics

- For most crackers, hacking is a personal lifestyle, a travel through technology.

- They are obsessive persons with an addiction to the thrill of hacking.

- They usually lack love and respect in their personal lives.

- They do not have a moral problem by crashing systems and stealing data and they might get recruited at the end by professional criminal organizations.

- When somebody shows respect for their amazing skills, they stop distrusting authority and displaying arrogance.

# Part 4

## ***Possible dangers***

# What’s the danger for the average computer user?

Most average computer users don’t have anything worth stealing...

So, what’s this all fuss about?

# *have you ever thought that:*

→→→ your computer could be
a launching pad for other attacks?

→→→ you could be accused of serious internet crimes you never commited?

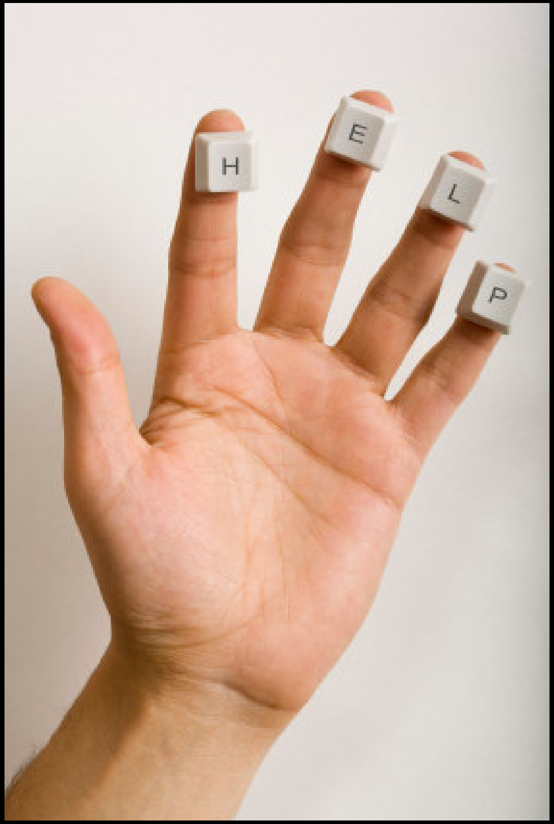
InfoSecurityLab

# Other possible dangers

- browsing into your files
- gaining access to your credit card numbers
- gaining access to your bank account
- entering web-sites using your password
- uploading or downloading any files from your computer
- deleting all the data and software on your computer

InfoSecurityLab

# So, you might need...



...with all these!

# Part 5

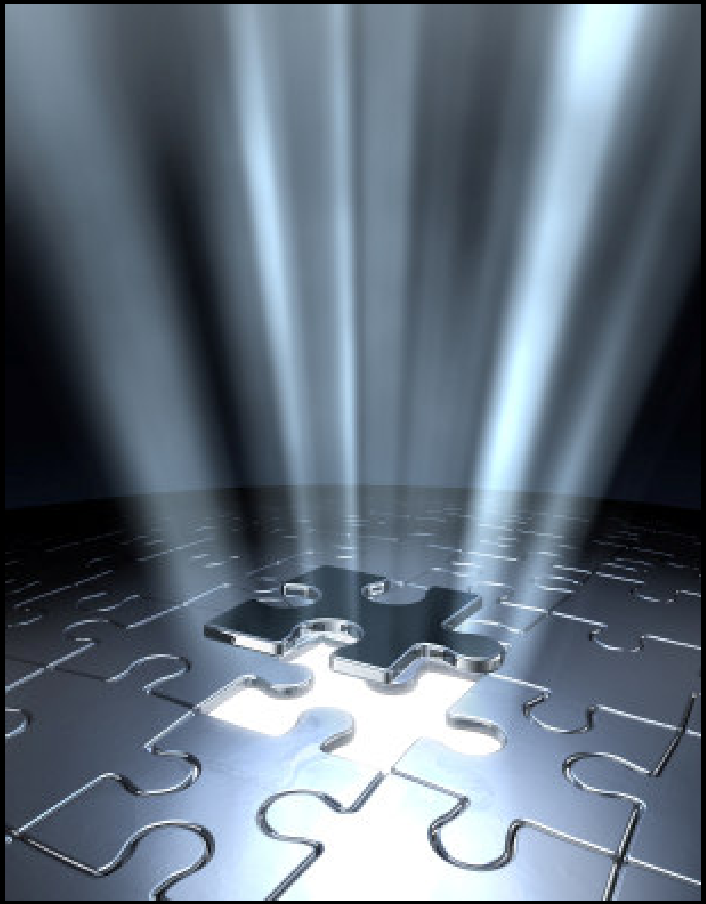
## ***Hackers' methodology***

# Crackers- their method 1

A specific methodology, developed over time, is being followed by crackers-hackers, and their way of thought is similar to computer developers.

Patience and careful movements in every step of their work is what characterizes their professionalism.

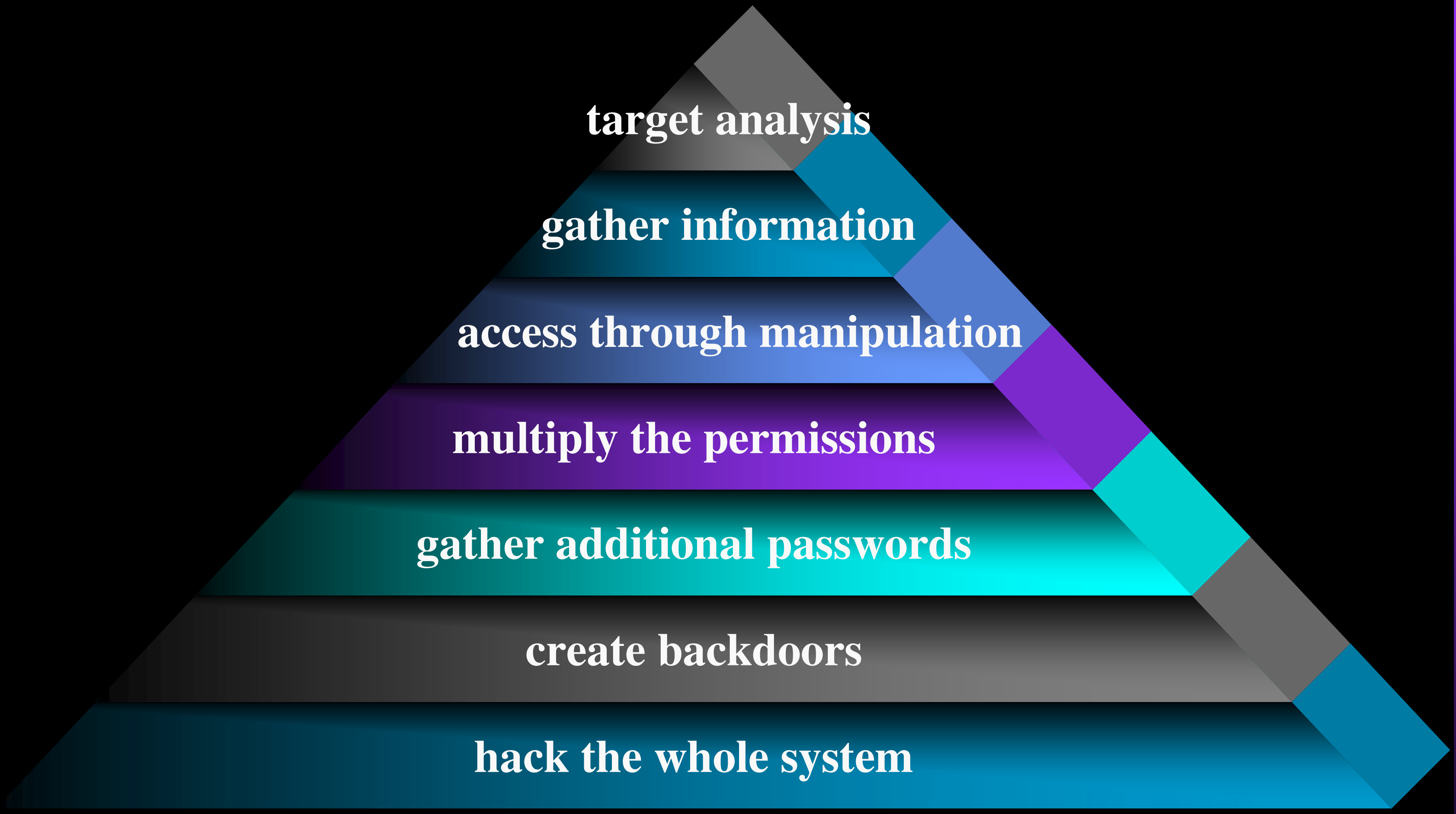
# Crackers- their method 2



They begin by knowing little or even no information about their target, but at the end of their investigation they will have constructed a detailed plan which leads to the defeat of the prey.

Their work is like solving a puzzle, with an easy, slow approach and extreme analysis.The soon-to-be-victim is the focus of their attention.

# 7 steps



target analysis

gather information

access through manipulation

multiply the permissions

gather additional passwords

create backdoors

hack the whole system

- *target analysis*

After the attacker identifies what he’s interested in, he performs a footprint analysis. His aim is to gather as much information as possible, so as to lay his scheme and to exclude all possibility of error. Usually, the usuful information during the attack includes:

- domain names
- phone numbers
- IP networks (internet protocol)
- other subsidiaries

- *gather information*

After generating a detailed roadmap, they enumerate the data which was obtained.

Now, the attacker is able to use all this information in order to reach his goal: to gain access to the system as an authenticated user!

The local administrators’ group is examined  and the easily guessed passwords are set on sight.

- ***access through manipulation***

THERE ARE 2 WAYS TO GET A PASSWORD FOR AN ACCOUNT OBTAINED IN THE PREVIOUS STEP:

- Social Engineering
- Brute Force Attack

- SOCIAL ENGINEERING

The attacker steals any ulitarian information by simulating an authorised user. The results are amazing... It's unbelievable what an unsuspecting employee will do for someone who seems or sounds authoritative!

- BRUTE FORCE ATTACK

  If the previous approach doesn't work, then the attacker tries to contact:

  (Network basic input/output system (NetBIOS) over TCP (TCP 139),Direct Host (TCP 445),Lightweight Directory Access Protocol (LDAP), (TCP 389),FTP (TCP 21),Telnet (TCP 23),Simple Network Management Protocol (SNMP), (UDP 161),Point-to-Point Tunneling Protocol (PPTP), (TCP 1723),Terminal Services (TCP 3389), so as to search for potential passwords and pair them with the already found usernames.

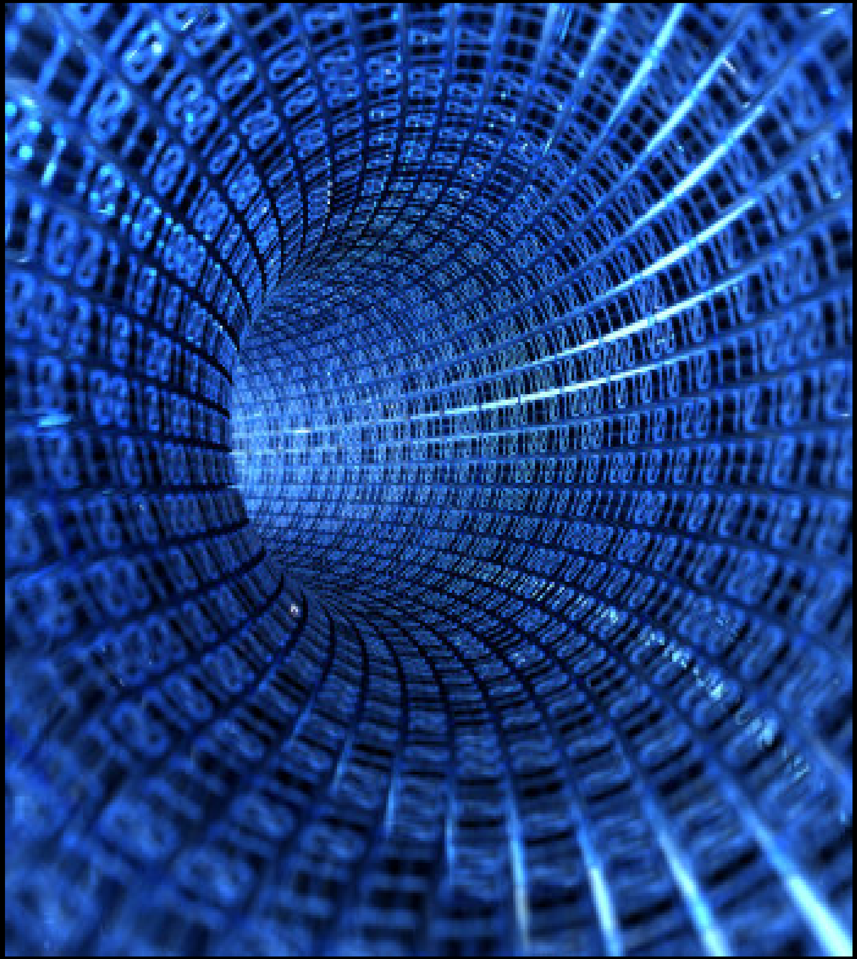
- *multiply the permissions*

When they have obtained user-level privileges from a host, they will definately try to escalate their permissions by scanning all information on the host. They will review:

- Batch files, which contain hardcored usernames and passwords
- Registry keys, which lead to applications or usernames’ passwords
- E-mails and documents, which can provide additional information for other systems on the network

Sometimes, the attacker infects using the *trojan* system too, which means that he copies malicious code to the user’s system and gives it the same name as frequently used pieces of software.

- *gather additional passwords*



Using tools like Pwdump2 and Lsadump2, the crackers take absolute control of all computers in the hacked network, just by logging in this system with administrative credentials.

- *create backdoors*

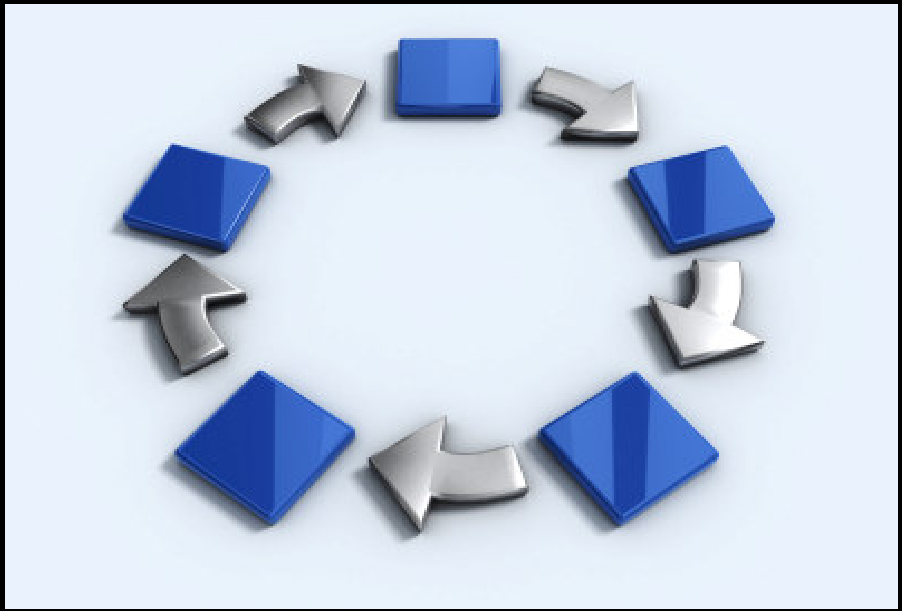
In the case that a cracker has to leave the computer immediately, so as not to be caught, he installs backdoors. It means that he will create a way in which he will be able to access the system remotely. If there are strong router filtering or firewalls, then he needs to use more complex backdoors, like reverse trafficking. This enables him to execute code on the protected computer.

- *hack the whole system*

Port redirectors, that are also being created, help bypass the port filters, routers and firewalls and generally they help in avoiding the intrusion detection devices.

After creating port directors and backdoors, the attacker can move on hacking other systems on network apart from the local one.

As each system is hacked, the cracker repeats all steps which have been mentioned and in this way he can break into a lot of systems and gain administrator’s access.



Unless he gets caught before this, it’s almost impossible to oust him from the network.

# Part 6

## ***Latest methods of hacking***

# *Hacking with software agents*

One of the newest methods in the area of hacking is using software agents, based on the technology of intelligent agents.

These software agents –interesting pieces of code, like *YAWATT*, *httpbee and pbounce*- provide: autonomous functionality

- cooperation capabilities
- quick learning from human activity
- capabilities and large amounts of data
- ability to analyze themselves in terms of behavior, error and success

# ***As a result:***

- hacking is done in a faster way
- uncertainty is dealt with in an intelligent way.

# Part 7

## ***Script Kids***

InfoSecurityLab

# Script kiddies

This is another possible danger that can attack your computer. And it’s just...

KIDS!

- usually adolescent boys
- feel bored, lonely and usually social outcasts
- they brag about damaging other people’s computers by using trojans, but generally they have no great knowledge of computers
- they merely run scripts (programmes, code), which are written by other crackers-hackers and they feel they gain a sense of worth by ruining somebody’s files

***They are also called script bunnies, script kitties or skiddies.***

# Part 8

## ***How to protect***

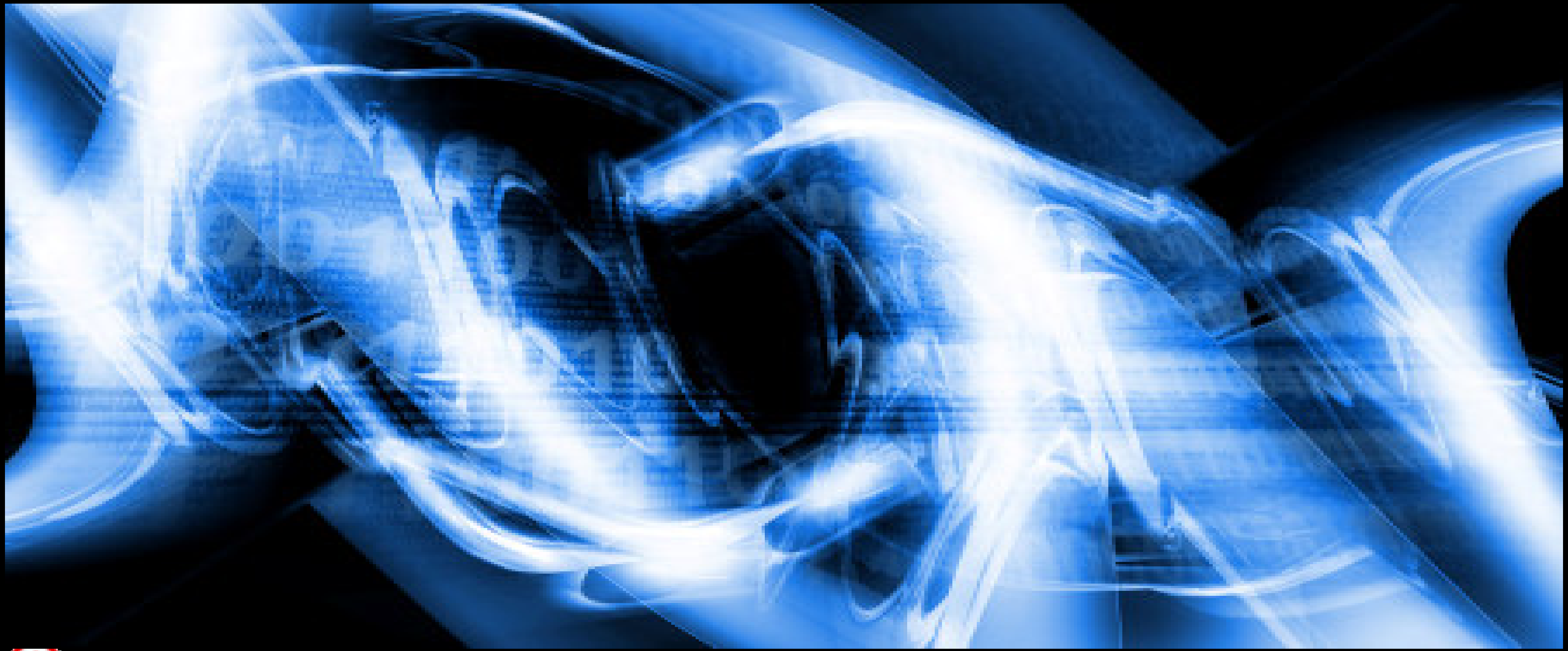
# Protection

So as to be aware of the possible danger, we just have to know the best possible ways of protection. In this case, crackers' attacks can be defeated by:

- *operating systems updates*
- *anti-virus software*
- *firewall software*
- *e-mail filtering & software preview windows*

- ***operating systems updates***

As a part of our daily routine, we should get used to apply regularly updates and patches, and download any critical security updates.



- *anti-virus software*

A reliable anti-virus software is vital for our computer and it would be even more trustworthy if we set passwords to protect the settings of it. Updating the anti-virus is also very important.

## •*firewall software*

A firewall software prevents unauthorized incoming and outcoming communication from the computer, while it’s connected to the internet.

It blocks unwanted inbound traffic as well as outbound traffic, so that trojan or spyware can’t give authority to any cracker who wants to take control of the computer.

- *e-mail filtering & software preview windows*

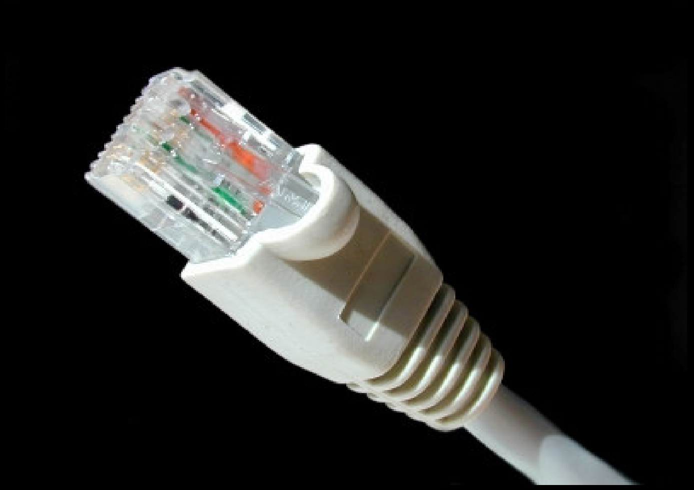
Filtering the e-mails even before they are collected into the mail-box, is very important for the safety of our computer.

Spam and virus-containing e-mails, are reported as junk and we save time and bandwidth used while retrieving our mail.

Furthermore, it’s wiser to turn off the preview window(if it’s a handy feature), so as to avoid worms activating our system. Worms could transmit our files throughout the internet, even if we didn’t click on the attachments of the e-mail.

# Extra advices

- Disconnect your computer from the internet while not using it.



- In case there are some more people using your personal computer, don’t allow any software to be installed without your permission.

- Insure your passwords are highly protected and not easily guessed.

- Log out of online services right after you finish your job.

- Supervise your kids while surfing the net. They have little idea about security in chat rooms and this could end up in a disaster.

# Part 9

*We can beat them*

# Crackers are not undefeated

The world of information may help the growth of immoral activities, such as cracking-hacking, but it also help us to understand the nature of all these attacks and prevent them.

# ***So, be aware and save your privacy.***

Knowledge is our treasure and we shall take advantage of every new tool against this violation of our private life.