

# Computer Security

- Computer Security is the process of detecting and preventing any unauthorized use of your laptop/computer.
- It involves the process of safe guard against for who enter with out permission from using your personal or office based computer resources with malicious intent or even for gaining any access to them accidentally.

# Goals of Computer Security

## Integrity:

- Guarantee that the data is what we expect

## Confidentiality

- The information must just be accessible to the authorized people

## Reliability

- Computers should work without having unexpected problems

## Authentication

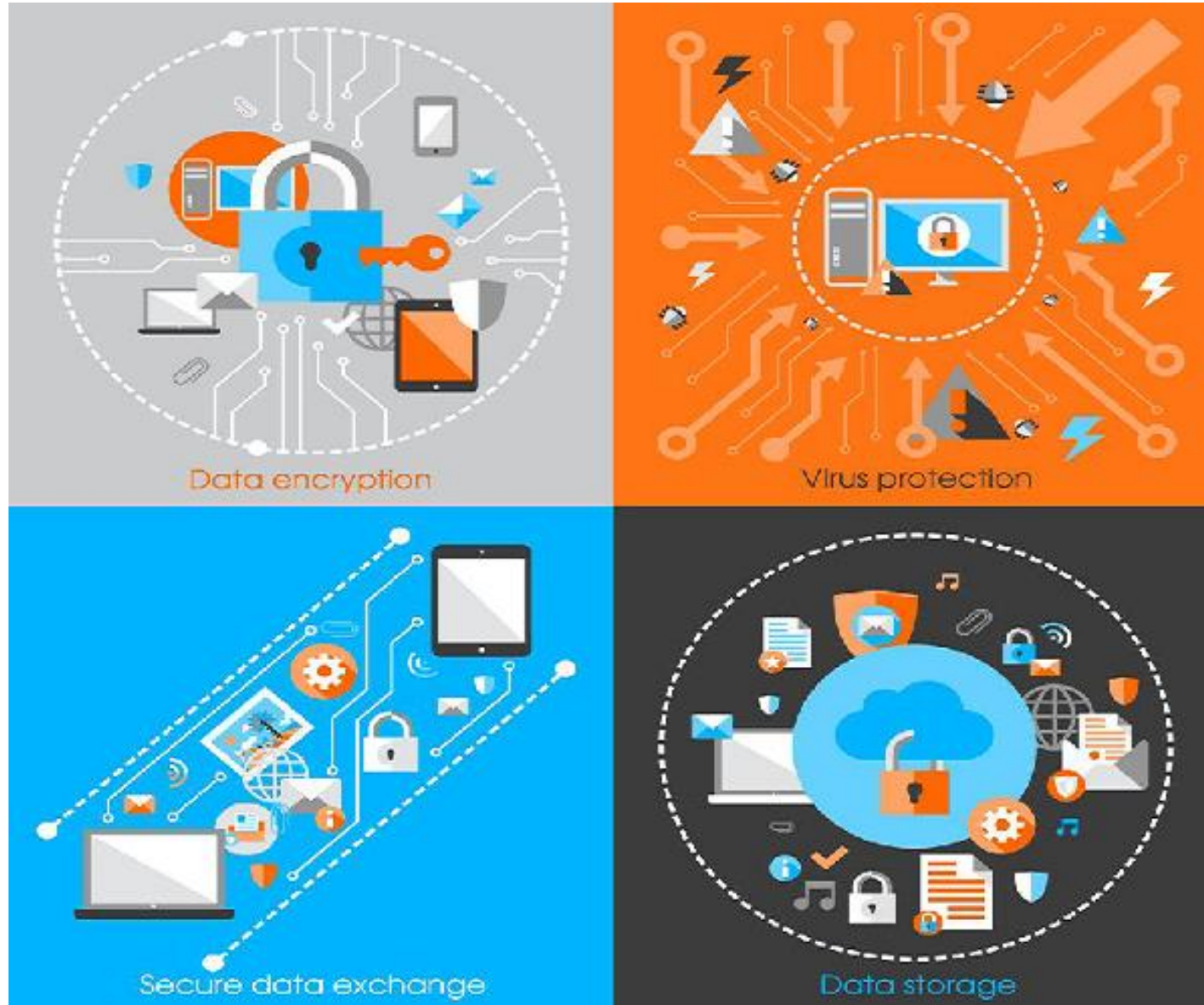
- Guarantee that only authorized persons can access to the resources

# Why Security

One important indicator is the IT skills of a person that wants to hack but the success rate of it has increased, this is because of three main factors –

- Hacking tools that can be found very easily by everyone just by googling and they are endless.
- Technology with the end-users has increased within these years, like internet bandwidth and computer processing speeds.
- Access to hacking information manuals.

# What to Secure



point of what all to secure in a computer environment –

- First of all, is to check the physical security by setting control systems like motion alarms, door accessing systems, humidity sensors, temperature sensors. All these components decrease the possibility of a computer to be stolen or damaged by humans and environment itself.
- People having access to computer systems should have their own user id with password protection.

# Conti...

- Monitors should be screen saver protected to hide the information from being displayed when the user is away.
- Secure your network especially wireless, passwords should be used.
- Internet equipment as routers to be protected with password.
- Data that you use to store information which can be financial, or non-financial by encryption.

# Potential Losses due to Security Attacks

- **Losing you data** – If your computer has been hacked .
- **Bad usage of your computer resources** – Your network or computer can go in overload so you cannot access your services .It can be used by the hacker to attack another machine or network.
- **Reputation loss** – Just think if your Facebook account or business email has been owned by a social engineering attack and it sends fake information to your friends.
- **Identity theft** – This is a case where your identity is stolen (photo, name surname, address, and credit card) and can be used for a crime like making false identity documents.

# Basic Computer Security Checklist


There are some basic things that everyone of us in every operating system need to do –

- Check if the user is password protected.
- Check if the operating system is being updated.



screenshot of laptop which is a Windows 7.


Windows Update



**Install updates for your computer**

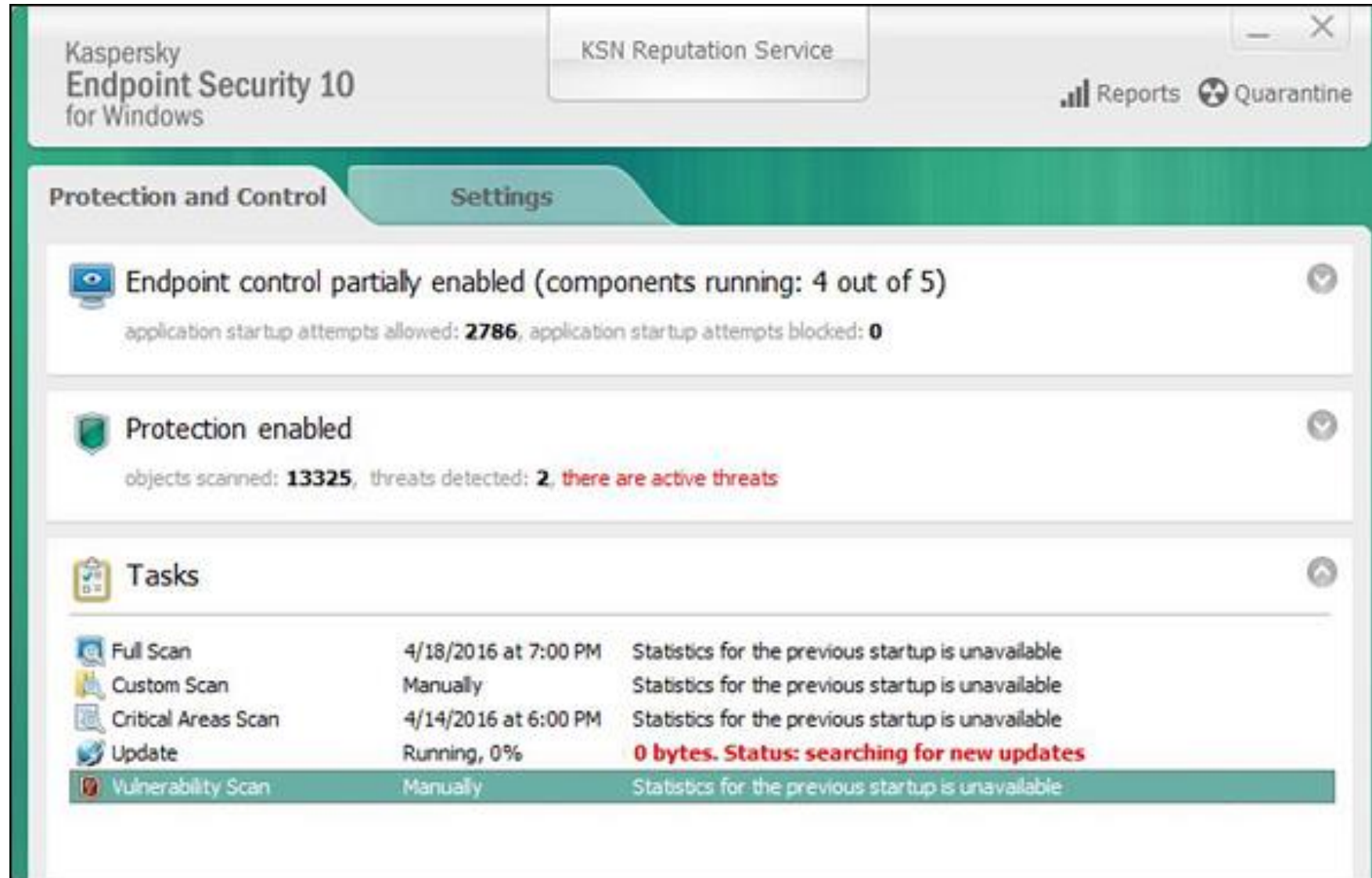
1 important update is available  
11 optional updates are available

**1 important update selected, 44.9 MB**

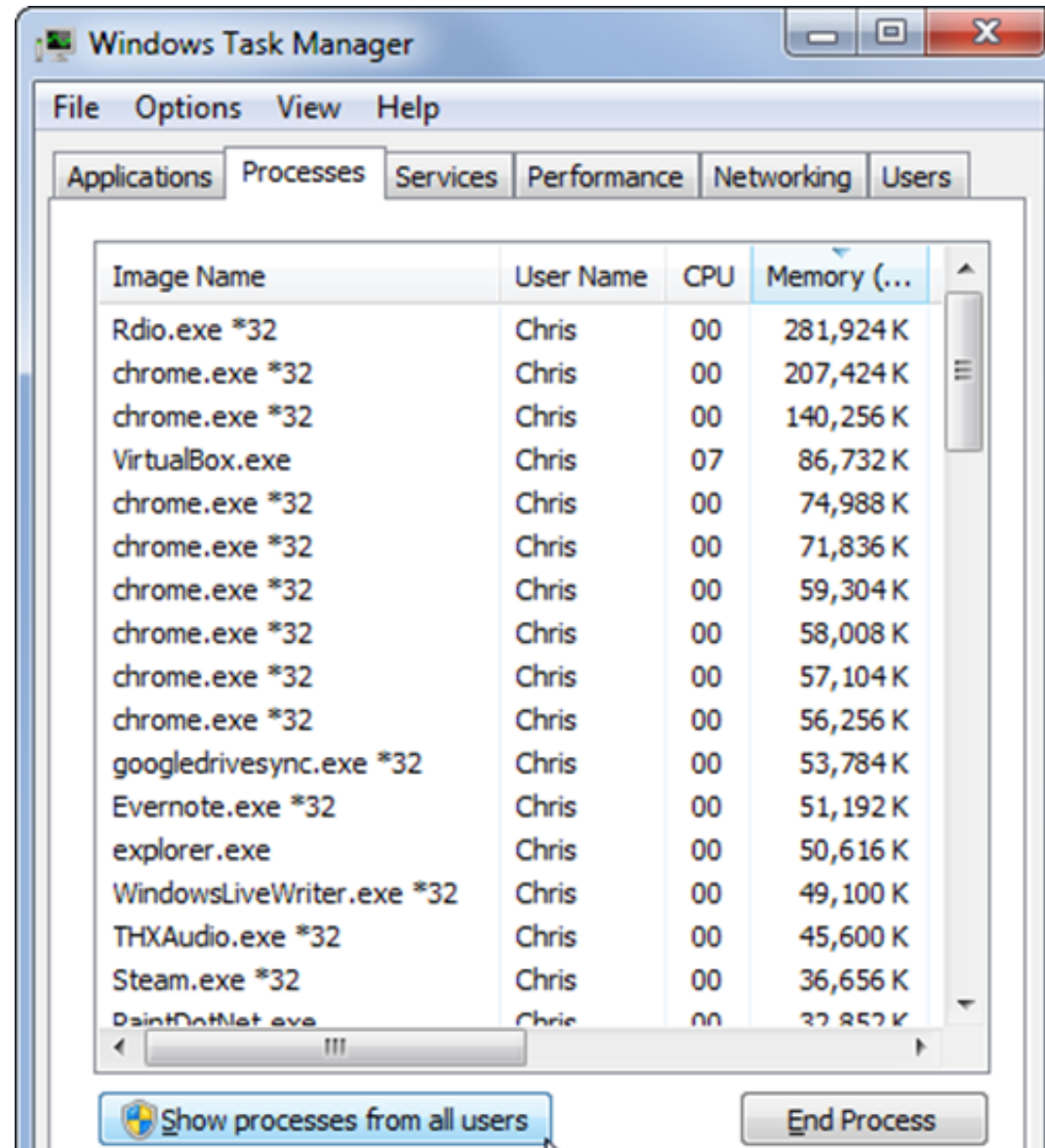
 **Install updates**

Most recent check for updates: Today at 9:14 AM  
Updates were installed: Today at 8:29 AM. [View update history](#)  
You receive updates: For Windows and other products from Microsoft Update

Check if the antivirus or antimalware is installed and updated.  
Kaspersky antivirus being updated



Check for the unusual services running that consumes resources



- Check if your monitor is using a screen saver.
- Check if the computer firewall is on or not.
- Check if you are doing backups regularly.
- Check if there are shares that are not useful.
- Check if your account has full rights or is restricted.
- Update other third party software's.

# Different terminology used in Computer Security.

- **Unauthorized access** – An unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details.
- **Hacker** – Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.
- **Threat** – Is an action or event that might compromise the security.
- **Vulnerability** – It is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system.

- **Attack** – Is an assault on the system security that is delivered by a person or a machine to a system. It violates security.
- **Antivirus or Antimalware** – Is a software that operates on different OS which is used to prevent from malicious software.
- **Social Engineering** – Is a technique that a hacker uses to stole data by a person for different for purposes by psychological manipulation combined with social scenes.
- **Virus** – It is a malicious software that installs on your computer without your consent for a bad purpose.
- **Firewall** – It is a software or hardware which is used to filter network traffic based on rules.

# Security Basics

- Types of Security
  - Network Security
  - System and software security
  - Physical Security
- Very little in computing is secure, you must protect yourself!
  - Software cannot protect software
  - Networks can be protected better than software

# Some Types of Attacks

What are some common attacks?

- Network Attacks

Packet sniffing, man-in-the-middle, DNS hacking

- Web attacks

Phishing, SQL Injection, Cross Site Scripting

- OS, applications and software attacks

Virus, Trojan, Worms, Rootkits, Buffer Overflow

- Social Engineering

(NOT social networking)



# Network Attacks

## Packet Sniffing

- Internet traffic consists of data “packets”, and these can be “sniffed”
- Leads to other attacks such as password sniffing, cookie stealing session transit, information stealing



## Man in the Middle

- Insert a router in the path between client and server, and change the packets as they pass through

## DNS transit

- Insert malicious routes into DNS tables to send traffic for genuine sites to malicious sites

# Web Attacks

## Phishing

- An evil website pretends to be a trusted website
- Example:
  - You type, by mistake, “mibank.com” instead of “mybank.com”
  - mibank.com designs the site to look like mybank.com so the user types in their info as usual
  - BAD! Now an evil person has your info!

## SQL Injection

- Interesting [Video](#) showing an example

## Cross Site Scripting

- Writing a complex Javascript program that steals data left by other sites that you have visited in same browsing session

# OS, applications and software attacks

## Virus

- Definition

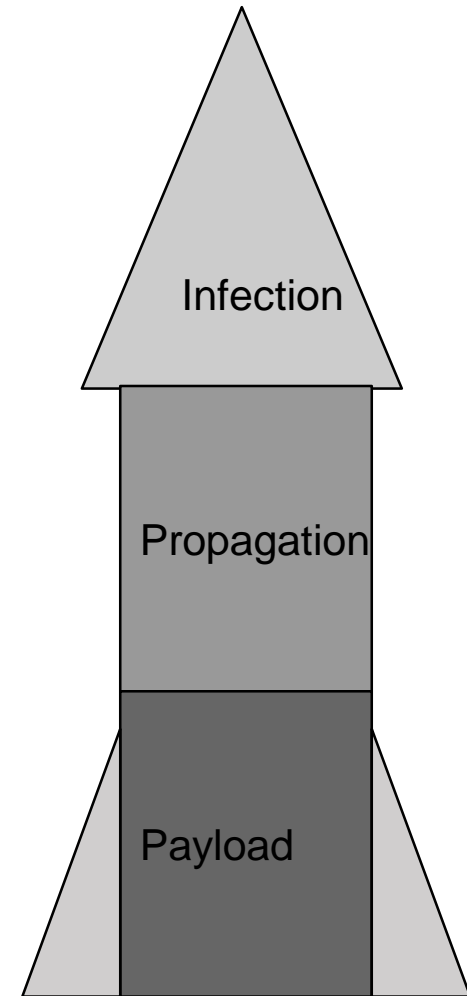
- Piece of code that automatically reproduces itself. It's attached to other programs or files, but requires user intervention to propagate.

- Infection (targets/carriers)

- Executable files
- Boot sectors
- Documents (macros), scripts (web pages), etc.

- Propagation

is made by the user. The mechanisms are storage elements, mails, downloaded files or shared folders



# Worm

## Definition

- Piece of code that automatically reproduces itself over the network. It doesn't need the user intervention to propagate (autonomous).

## Infection

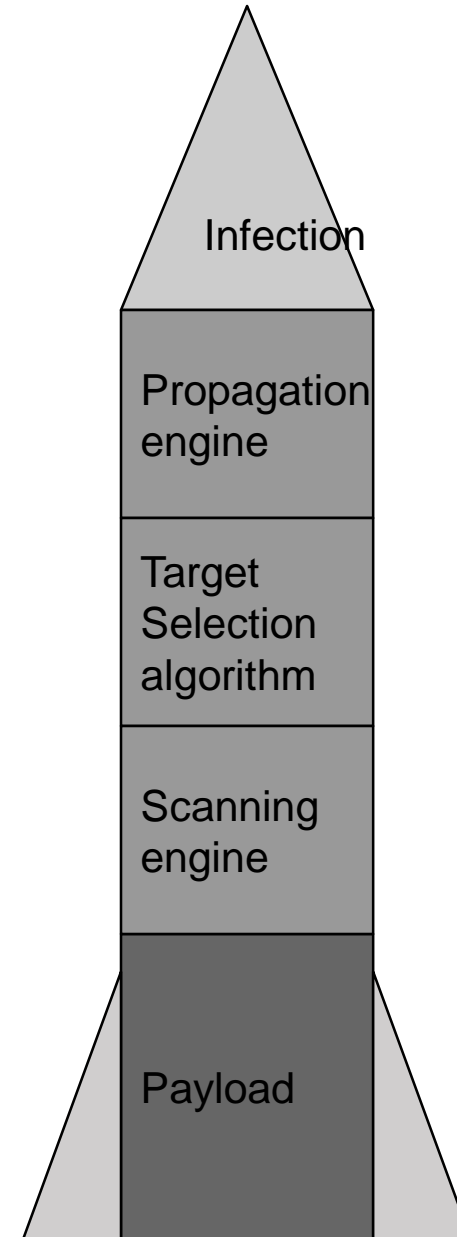
- Via buffer overflow, file sharing, configuration errors and other vulnerabilities.

## Target selection algorithm

- Email addresses, DNS, IP, network neighborhood

## Payload

- Malicious programs
- Backdoor, DDoS agent, etc.



# Backdoor, trojan, rootkits

## Goal

- The goal of *backdoor*, *Trojan* and *rootkits* is to take possession of a machine subsequently through an infection made via a backdoor.

- **Backdoor**

- A *backdoor* is a program placed by a black-hacker that allows him to access a system. A *backdoor* have many functionalities such as keyboard-sniffer, display spying, etc.



- **Trojan**

- A *Trojan* is a software that seems useful, but is actually hiding a malicious functionality.

- **Rootkits (the ultimate virus)**

- *Rootkits* operate like *backdoor* and *Trojan*, but also modify existing programs in the operating system. That allows a black-hacker to control the system without being detected. A *rootkit* can be in user-mode or in kernel-mode.



# Social Engineering

- Why is this social engineering?
  - Manipulating a person into divulging confidential information
- I am not dumb, so does this really apply to me?
  - YES! Attackers are ALSO not dumb.
  - Social Engineers are coming up with much better and much more elaborate schemes to attack users.
  - Even corporate executives can be tricked into revealing VERY secret info
- What can I do to protect myself?
  - NEVER give out your password to ANYBODY.
  - Any system administrator should have the ability to change your password without having to know an old password

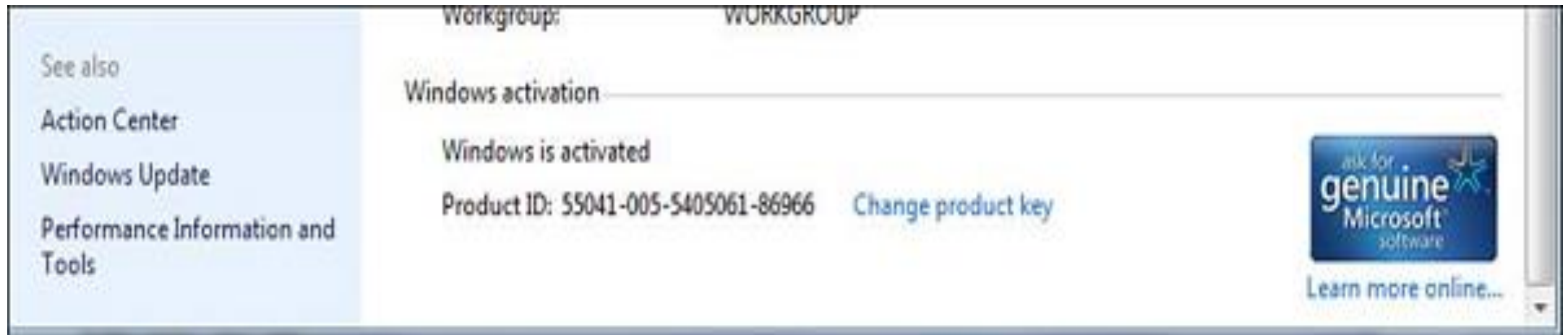
# Password Attacks

- Password Guessing
  - Ineffective except in targeted cases
- Dictionary Attacks
  - Password are stored in computers as hashes, and these hashes can sometimes get exposed
  - Check all known words with the stored hashes
- Rainbow Tables
  - Trade off storage and computation – uses a large number of pre-computed hashes without having a dictionary
  - Innovative algorithm, that can find passwords fast!
    - e.g. 14 character alphanumeric passwords are found in about 4-10 minutes of computing using a 1GB rainbow table

# Guidelines for Windows OS Security

Following are the list of guidelines for Windows Operating System Security.

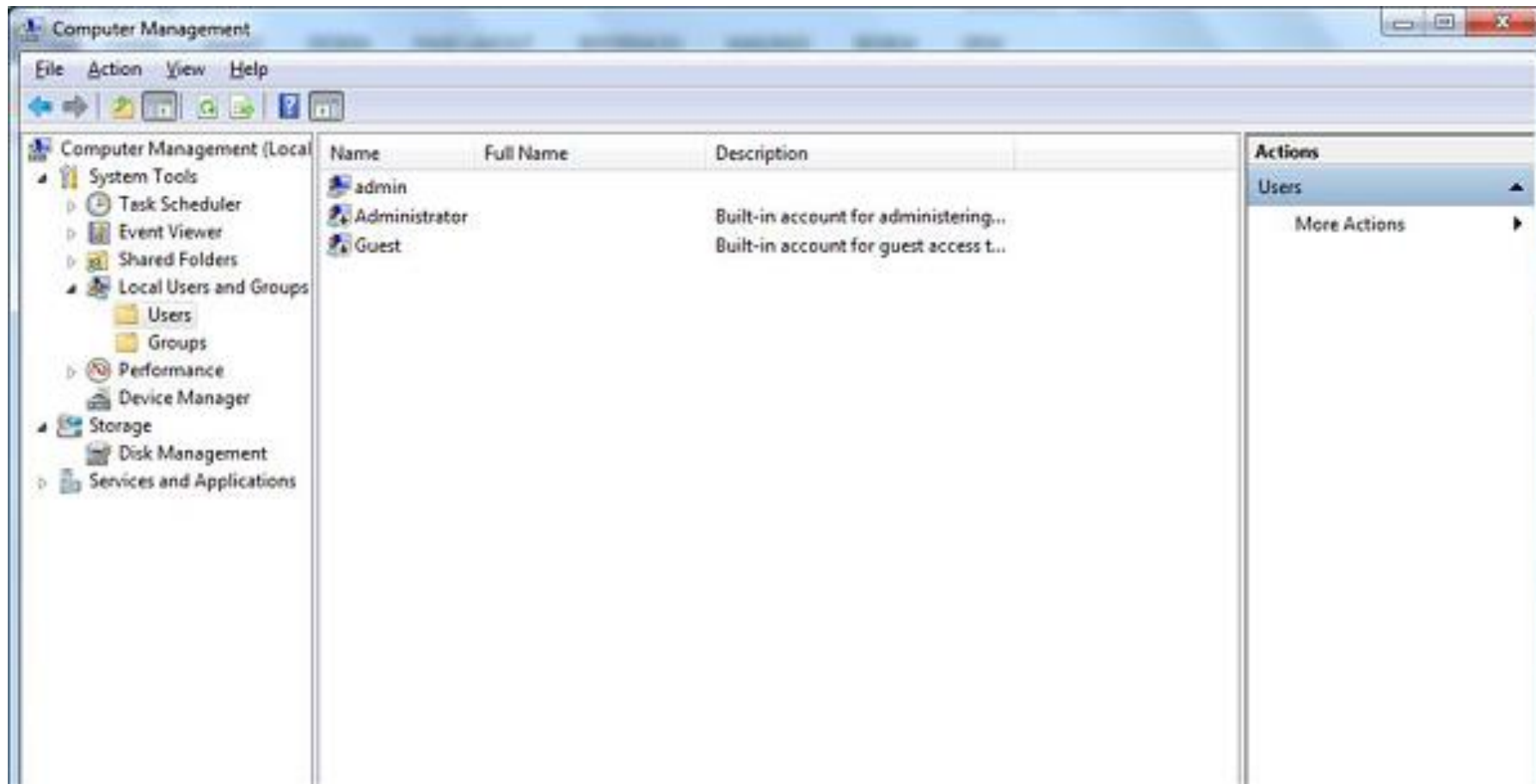
**01. Use the licensed versions of Windows OS**, not the cracked or pirated ones and activate them in order to take genuine updates.





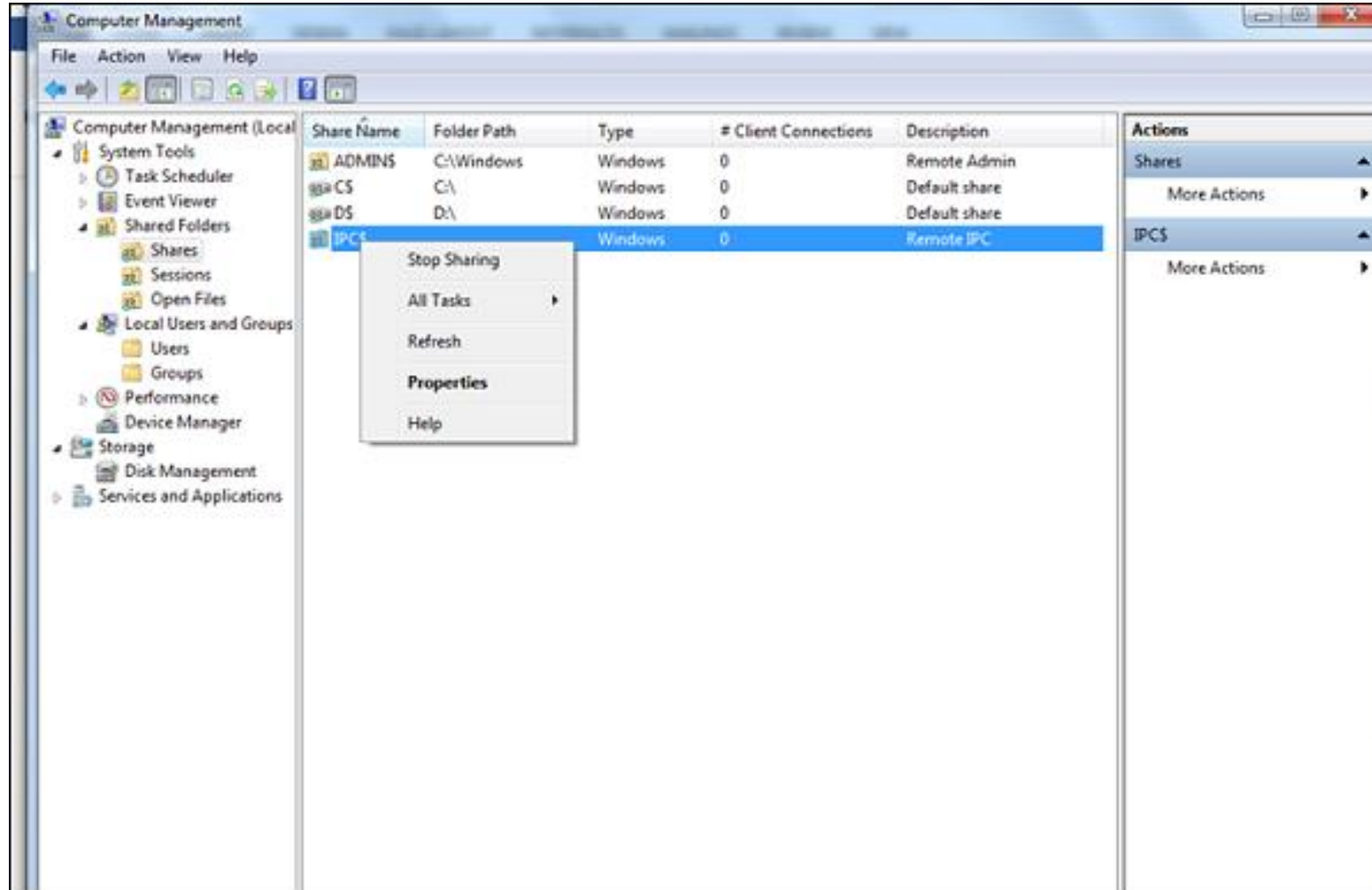
## 02.Disable Unused Users

- To do this, Right Click on Computer – Manage – Local Users and Groups – Users, then disable those users that are not required.



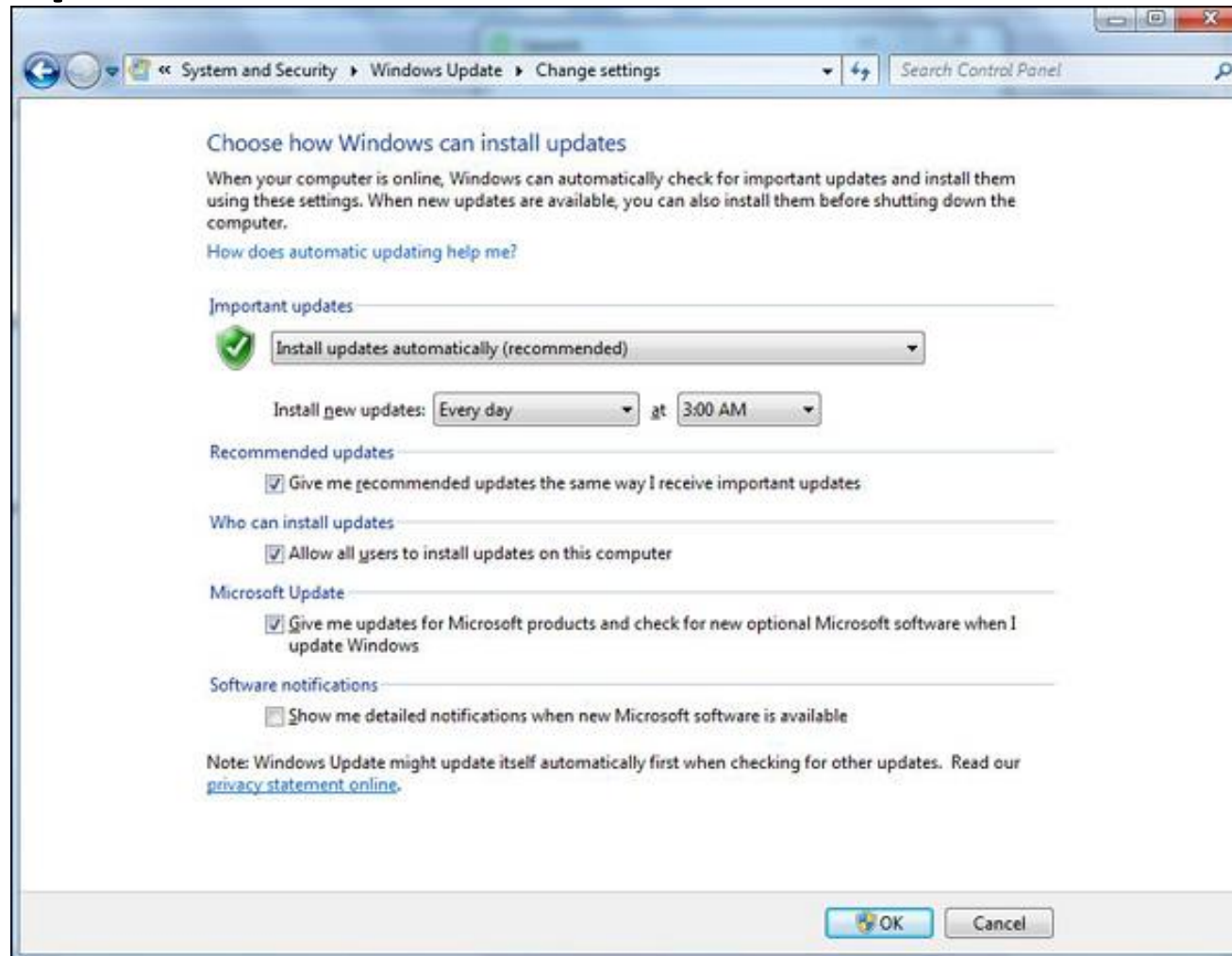
# 03.Disable unused shares

- Right Click on My Computer – Manage – Shared Folders – Right Click Stop Sharing.



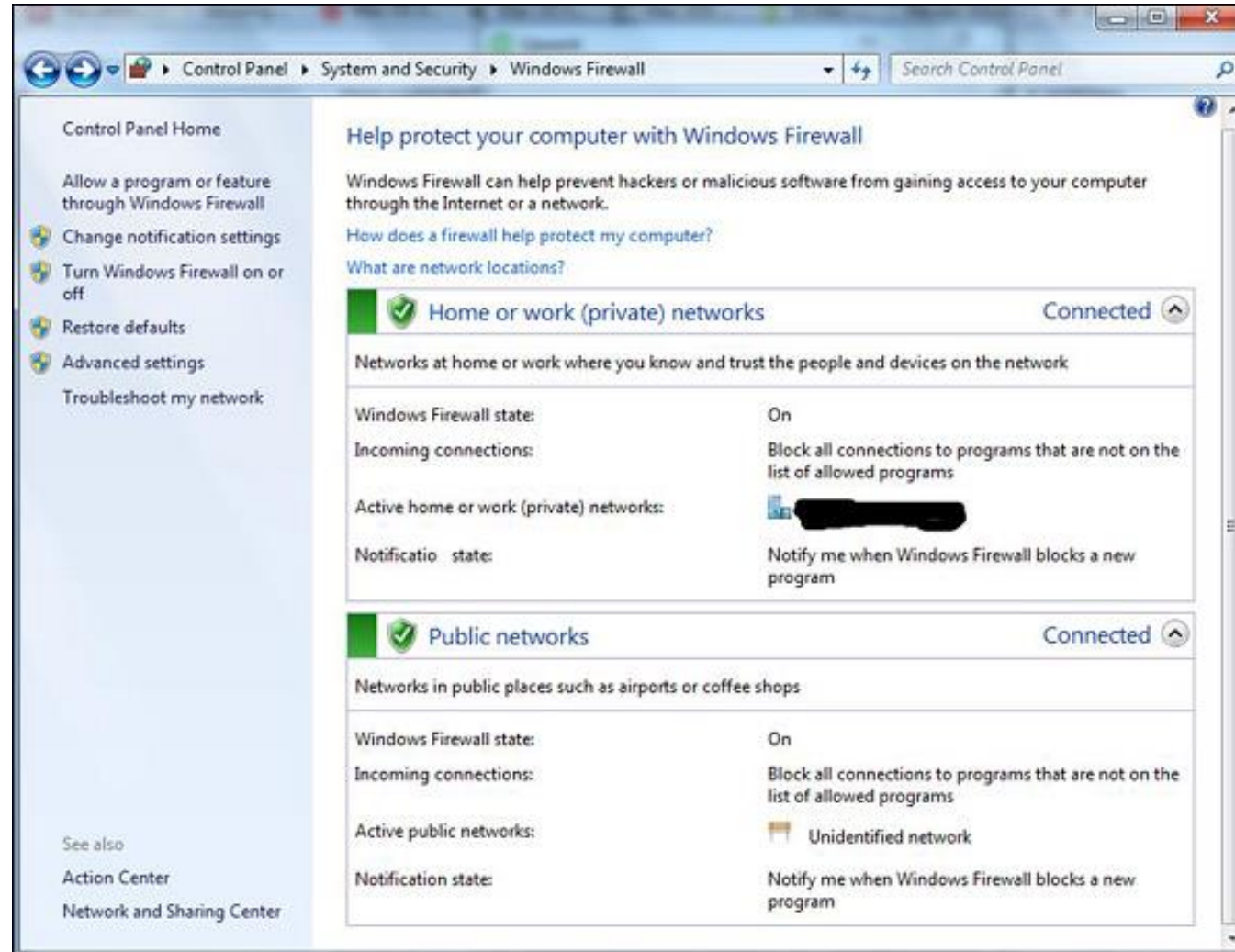
# 04.updates regularly for Windows OS

To set this up, go to **Control Panel – System and Security – Windows Updates – OK.**



## 05.Windows System Firewall up

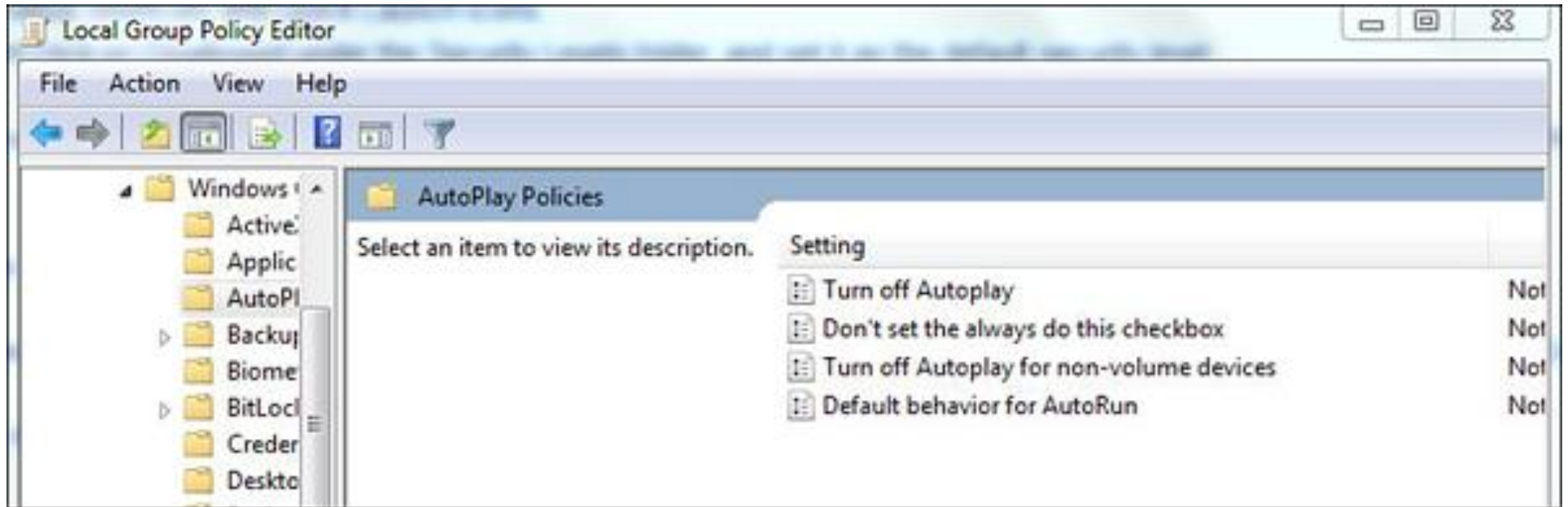
- To set this up, go to **Control Panel – System and Security – Windows Firewall.**



## 06. Disable Auto play for Removable Media.

This blocks the viruses to run automatically from removable devices.

- **Start – on Search box type Edit Group Policy –Administrative Templates – Windows Components – Autoplay Policy – Turn off Autoplay – Enable – Ok.**



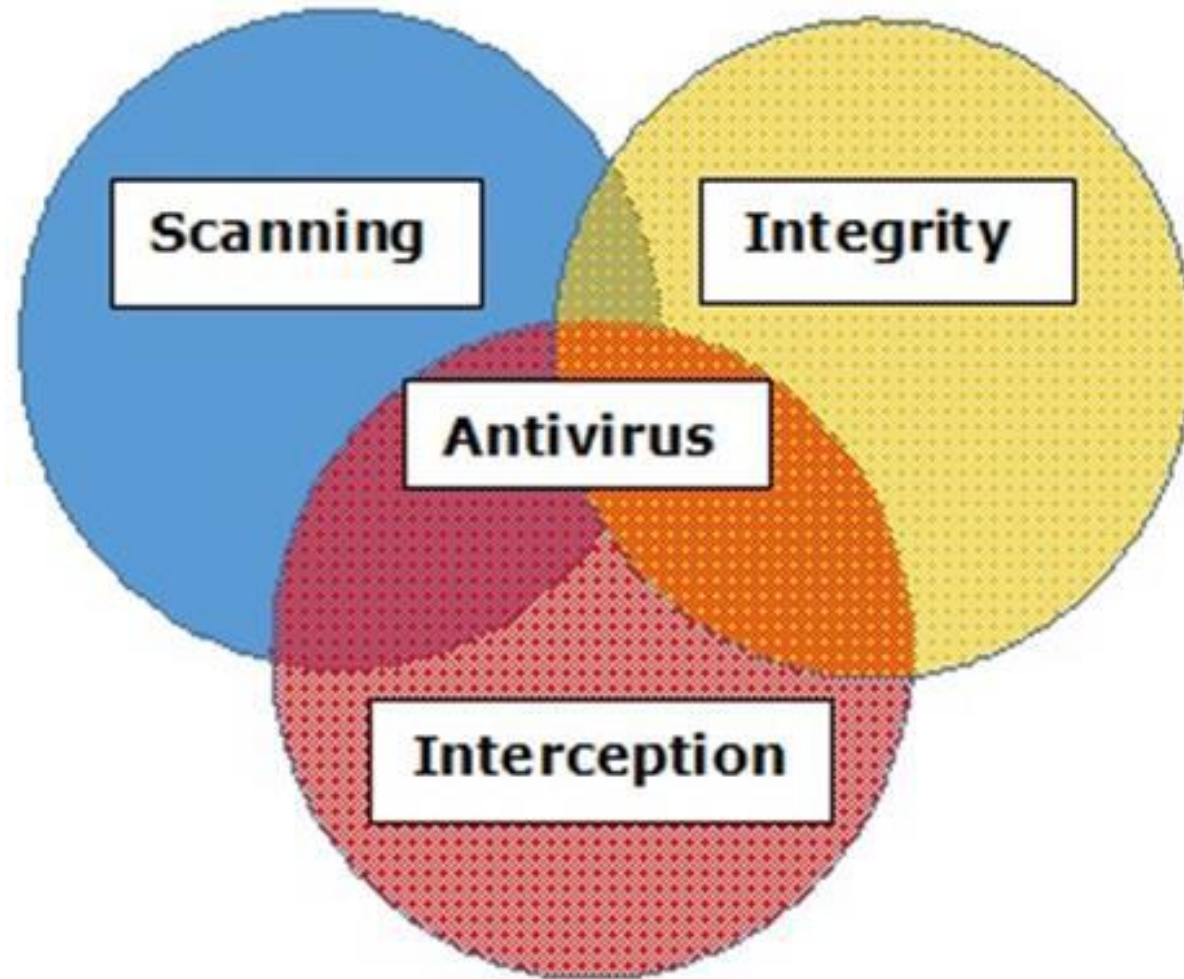
# Basic Functions of Antivirus Engines

All antivirus engines have three components to function accordingly. It is important to have a look at these functions because it will help us for better manual cleaning of viruses in case we need.

- **Scanning** – When a new virus is detected in the cyberspace, antivirus producers start writing programs (updates) that scans for similar signature strings.
- **Integrity Checking** – This method generally checks for manipulated files in OS from the viruses.
- **Interception** – This method is used basically to detect Trojans and it checks the request made by the operating system for network access.



The following image shows the schema for an antivirus engines functionality.



# Computer Security Issues

- **Vulnerability** is a point where a system is susceptible to attack.
- A **threat** is a possible danger to the system. The danger might be a person (a system cracker or a spy), a thing (a faulty piece of equipment), or an event (a fire or a flood) that might exploit a vulnerability of the system.
- **Countermeasures** are techniques for protecting your system



# Vulnerabilities in Systems

- How do viruses, rootkits enter a system?
  - Even without the user doing something “stupid”
- There are vulnerabilities in most software systems.
  - Buffer Overflow is the most dangerous and common one
- How does it work?
  - All programs run from memory.
  - Some programs allow access to reserved memory locations when given incorrect input.
  - Hackers find out where to place incorrect input and take control.
  - Easy to abuse by hackers, allows a hacker complete access to all resources

# How can you achieve security?

- Many techniques exist for ensuring computer and network security
  - Cryptography
  - Secure networks
  - Antivirus software
  - Firewalls
- In addition, users have to practice “safe computing”
  - Not downloading from unsafe websites
  - Not opening attachments
  - Not trusting what you see on websites
  - Avoiding Scams

# Why Care?

- Online banking, trading, purchasing may be insecure
  - Credit card and identity theft
- Personal files could be corrupted
  - All school work, music, videos, etc. may be lost
- Computer may become too slow to run
  - If you aren't part of the solution you are part of the problem
- Pwn2Own contest - 2008
  - Mac (Leopard) fell first via Safari, Vista took time but was hacked via Flash Player, Ubuntu stood ground.
- Upon discovery, vulnerabilities can be used against many computers connected to the internet.

# Role of the Security Policy in Setting up Protocols

Some pointers which help in setting u protocols for the security policy of an organization.

- Who should have access to the system?
- How it should be configured?
- How to communicate with third parties or systems?

Policies are divided in two categories –

01. User policies

02. IT policies.

## **User policies**

generally define the limit of the users towards the computer resources in a workplace.

For example, what are they allowed to install in their computer, if they can use removable storages.

**IT policies** are designed for IT department, to secure the procedures and functions of IT fields.

- **General Policies** – This is the policy which defines the rights of the staff and access level to the systems. Generally, it is included even in the communication protocol as a preventive measure in case there are any disasters.

- **Server Policies** – This defines who should have access to the specific server and with what rights.
- **Firewall Access and Configuration Policies** – It defines who should have access to the firewall and what type of access, like monitoring, rules change. Which ports and services should be allowed and if it should be inbound or outbound.
- **Backup Policies** – It defines who is the responsible person for backup, what should be the backup, where it should be backed up, how long it should be kept.
- **VPN Policies** – These policies generally go with the firewall policy, it defines those users who should have a VPN access and with what rights. For site-to-site connections with partners, it defines the access level of the partner to your network.

# Types of Policies

most important types of policies

- **Permissive Policy** – It is a medium restriction policy where we as an administrator block just some well-known ports of malware regarding internet access and just some exploits are taken in consideration.
- **Prudent Policy** – This is a high restriction policy where everything is blocked regarding the internet access, just a small list of websites are allowed, and now extra services are allowed in computers to be installed and logs are maintained for every user.
- **Acceptance User Policy** – This policy regulates the behavior of the users towards a system or network or even a webpage, so it is explicitly said what a user can do and cannot in a system. Like are they allowed to share access codes, can they share resources, etc.

- **Information Protection Policy** – This policy is to regulate access to information, how to process information, how to store and how it should be transferred.
- **Remote Access Policy** – This policy is mainly for big companies where the user and their branches are outside their headquarters. It tells what should the users access, when they can work and on which software like SSH, VPN, RDP.
- **Firewall Management Policy** – This policy has explicitly to do with its management, which ports should be blocked, what updates should be taken, how to make changes in the firewall, how long should be the logs be kept.



- **Email Usage Policy** – This is one of the most important policies that should be done because many users use the work email for personal purposes as well. As a result information can leak outside. Some of the key points of this policy are the employees should know the importance of this system that they have the privilege to use.
- **Software Security Policy** – This policy has to do with the software's installed in the user computer and what they should have. Some of the key points of this policy are Software of the company should not be given to third parties. Only the white list of software's should be allowed, no other software's should be installed in the computer.