ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (959-963), Month: April - June 2015, Available at: www.researchpublish.com

Network Security: Attacks and Defence

MS. Masroor Jahan Mohd.Mubeen Ansari

ASM Institute of Management & Computer Studies (IMCOST), Thane Mumbai, University Of Mumbai, India

Abstract: **Network security is an important aspect in every field like government offices, Educational institute and any business organization. Network security is a challenging problem due to the complexity of underlying hardware, software, and network interdependencies as well as human and social factors. It involves decision making in multiple levels and multiple time scales, given the limited resources available to both malicious attackers and administrators defending networked systems. The resources vary from bandwidth, computing, and energy at the machine level to manpower and scheduling at the organizational level.Data security is the extreme critical factor in ensuring the transmission of information via the network. Threats to data privacy are powerful tools in the hands of hackers that could use the vulnerabilities of a network to corrupt, destroy and steal the sensitive information. There are more network security measure to protect the data from attackers like antivirus software, firewalls, cryptography etc. In this paper we study about various types of attacks on network security and how to handle or prevent this attack.**

Keywords: **Virus, Firewall, security, attacks, Hardware Firewalls, Antivirus software.**

I. INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Internet security is a tree branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. But now- a days, there are too much unethical practices in the form of attacks which are causing problems in the field of information technology. These attacks are sometimes in the form of malicious which enter the system by themselves without any knowledge of the user and sometimes in the form of unauthorized user who got the access computer system for the purpose of corrupting of stored data, to steal information or keep to keen eyes on users activity. some of the common forms of the Attacks are: computers virus, Spam pashing spyware ,Adware ,Hacking ,Cracking , etc .These threats are primarily present due to the ignorance shown by the users, weak technology and bad design of the network .To protect data from such network viruses one of the network security measure is antivirus programmed. When considering network security, it must be emphasized that the all network secure. Network security not only concerns the security in the computers at each end of the communication channel.

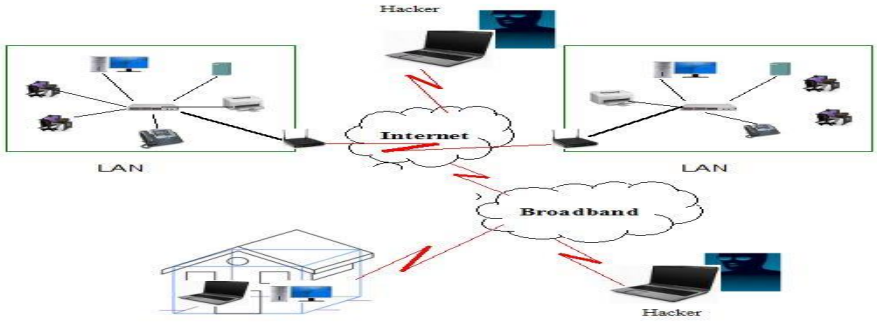

Fig 1. Network Security

Virus: A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, logging, or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.Virus(Vital Information Resource Under siege): Computer Virus are the malicious programs Having the ability to replicate and show themselves. They can attach themselves to the Programmed, files or data stored in the system automatically without any knowledge from the User. it can enter in a computer by different means like when one copy some dada from the virus Infected system to another uninfected system or while downloading some programs from the Internet or it can enter to system as an e-mail message's computer virus spread itself from One computer to another and interferences with the normal operations of a computer. Viruses attach themselves to any kind of .exe and .sys file, causing the unusual behavior of the programs or some time causing system crash.

II. TYPES OF NETWORK THREATS AND ATTACKS

As the types of threats, attacks, and exploits grow, various terms have been used to describe the individuals involved. Some of the most common terms are as follows:

a. White hat- These are network attackers who looks for vulnerabilities in systems or networks and then reports these vulnerabilities to the owners of the system so that they can be fixed. They are ethically opposed to the abuse of computer systems. A white hat generally focuses on securing IT systems.

b. Hacker- This is a general term that is used to describe a computer programming expert. These are normally used in a negative way to describe an individual that attempts to gain unauthorized access to network resources with malicious intent.

c. Black hat or Cracker- The opposite of White Hat, this term is used to describe those individuals who use their knowledge of computer systems and programming skills to break into systems or networks that they are not authorized to use, this of course is done usually for personal or financial gain.

d. Phreaker- This term is often used to describe an individual who manipulates the phone network in a bid to perform a function that is not allowed. The phreaker breaks into the phone network, usually through a payphone, to make free or illegal long distance calls.

e. Spammer- This is often used to describe the persons who sends large quantities of unsolicited e-mail messages. Spammers often use viruses to take control of home computers and use them to send out their bulk messages.

f. Phisher- Uses e-mail or other means to trick others into providing sensitive information, such as credit card numbers or passwords. A phisher masquerades as a trusted party that would have a legitimate need for the sensitive information.

III. PREVENTION MEASURES

1. Firewall:

Firewalls impose restrictions on incoming and outgoing Network packets to and from private networks. Incoming or outgoing traffic must pass through the firewall; only authorized traffic is allowed to pass through it. Firewalls create checkpoints between an internal private network and the public Internet, also known as choke points(borrowed from the identical military term of a combat limiting geographical feature). Firewalls can create choke points based on IP source and TCP port number. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network exposure by hiding the internal network system and information from the public Internet. Firewall software may require each individual user to make decisions about allowing or denying a program's requested access to the Internet (which helps prevent malware from sending proprietary information from your computer over the Internet, among other things). Users without much computer or security experience may be uncomfortable handling the requests and alerts that small business firewall software presents to them. Alternative solution is Network firewalls and Hardware Firewalls.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (959-963), Month: April - June 2015, Available at: www.researchpublish.com

1. a How to Secure Your Network with Windows Firewall:

A firewall is a hardware or software that monitors the traffic moving through a network gateway. Firewall can be configured to block or allow traffic based on defined criteria (ACLs). Firewalls blocks or allows random pings from a remote site to your computer or programs from your computer that attempts to access remote sites without your knowledge.

Most if not all windows software comes with inbuilt firewall. To view and configure your firewall on windows, follow these steps:

If your using XP

Single-click on the wireless connection icon in your system tray

Click Network and sharing centre

Click windows firewall

If you are using VISTA.

Click on start button

Right click on Network

Select Properties

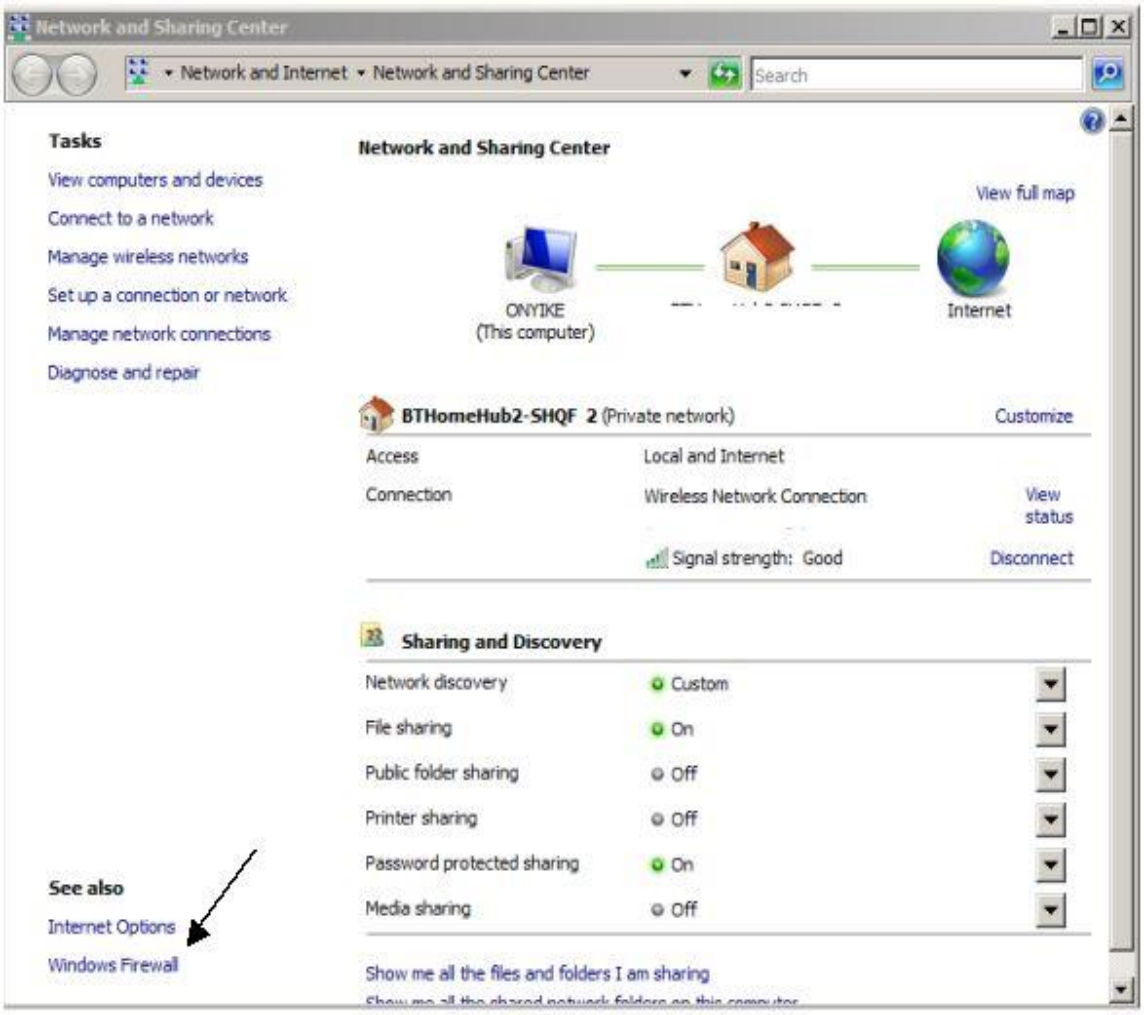

Fig 2. a. Firewall setting

Click on firewall

Click Turn Firewall On or Off

User account control dialogue box will appear, click Continue

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (959-963), Month: April - June 2015, Available at: www.researchpublish.com

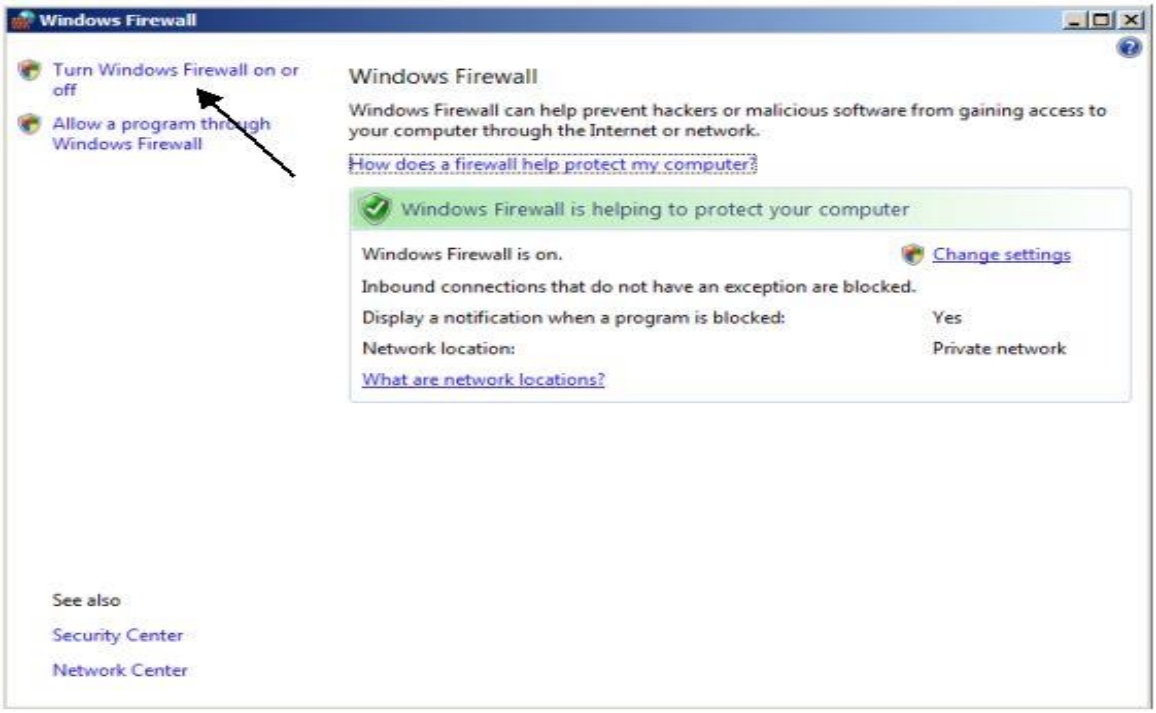

Fig.2.b. on

Click On

Click Apply

Then Click Ok

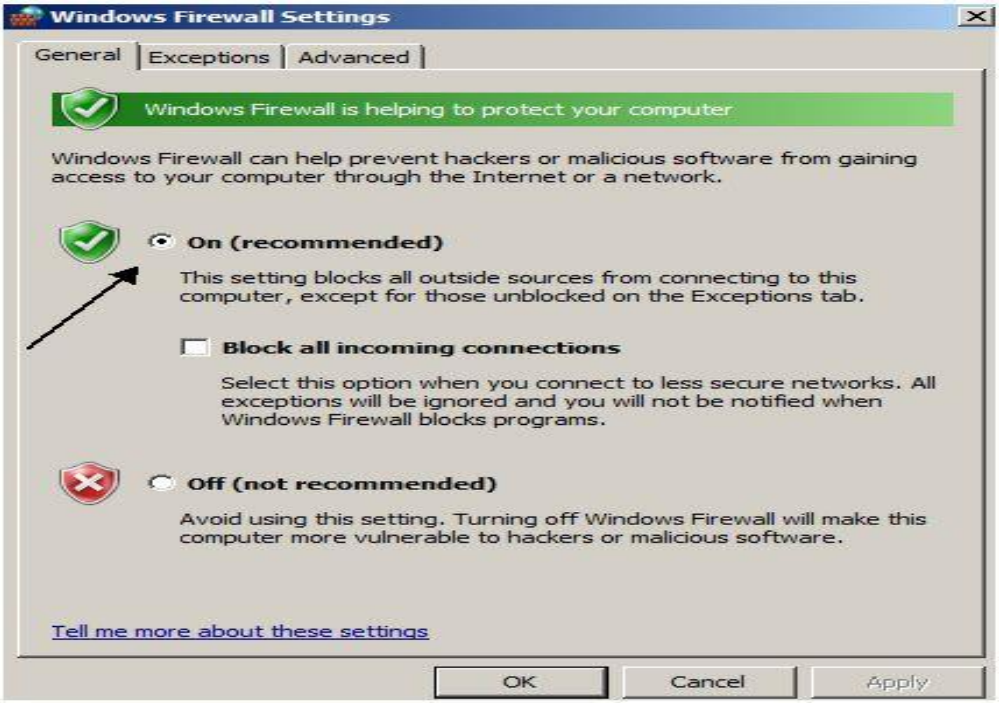

Fig.2.c. Successfully firewall applied

a. ***Network firewalls:***

It prevents unknown programs and processes from accessing the system. However, they are not antivirus systems and make no attempt to identify or remove anything. They may protect against infection from outside the protected computer or network, and limit the activity of any malicious software which is present by blocking incoming or outgoing requests

on certain TCP/IP ports. A firewall is designed to deal with broader system threats that come from network connections into the system and is not an alternative to a virus protection system.

b. Hardware Firewalls:

Hardware-based firewalls protect all the computers on your network. A hardware-based firewall is easier to maintain and administer than individual software firewalls. Hardware firewall integrated into a comprehensive security solution. In addition to a firewall, the solution should include virtual private network (VPN) support, antivirus, antispam, antispyware, content filtering, and other security technologies.

II. Antivirus:

Antivirus and Internet security programs can protect a programmable device from malware by detecting and eliminating viruses; Antivirus software was mainly shareware in the early years of the Internet, but there are now several free security applications on the Internet to choose from for all platforms .Antivirus software was originally developed to detect and remove computer viruses hence the name. Some Antivirus software also include protection from other computer thread, such as infected and malicious URL, spam, scan and pishing attacks, online identity (privacy), online banking attacks, social techniques, Advance Persistent Thread (APT),botnets DDoS attacks. Anti-virus programs are not always effective against new viruses because when antivirus scan the system and new virus are found then it take a time to update the virus database during this time virus get control over the system and hide themselves . The reason for this is that the virus designers test their new viruses on the major anti-virus applications to make sure that they are not detected before releasing them into the wild also one more reason is virus has used the Graphics Processing Unit (GPU) to avoid detection from anti-virus software. Some new viruses, particularly ransomware, use polymorphic code to avoid detection by virus scanners. This type of [ransomware virus] comes from sites that use a polymorphism. Even people having antivirus software running and it's not detecting anything. In this case usually people should reinstall the operating system or reinstall backups.

IV. CONCLUSION

Antivirus works on a very basic principle; they can scan a file and then matches, its digital signature against the known malwares. If the signature is match in the database is reports, delete it or even disinfect it depending on the clients setting. This system however easy has a huge drawback, whenever a new malware found ;it takes time before the antivirus database can be updated and during this period the malware can already take complete control of the system, disables the antivirus or even hides itself from the antivirus. To prevent this antivirus companies introduced a new system called online scanning and cloud antivirus. Cloud antivirus is a technology that uses lightweight agent software on the protected computer, while offloading the majority of data analysis to the provider's infrastructure. To implementing cloud antivirus involves scanning suspicious files using multiple antivirus engines which was an early implementation of the cloud antivirus concept called CloudAV. CloudAV was designed to send programs or documents to a network cloud where multiple antivirus and behavioural detection programs are used simultaneously in order to improve detection rates. Parallel scanning of files using potentially incompatible antivirus scanners is achieved by spawning a virtual machine per detection engine and therefore eliminating any possible issues. CloudAV is a solution for effective virus scanning on devices that lack the computing power to perform the scans themselves .In online scanning to maintain websites with free online scanning capability of the entire computer, critical areas only, local disks, folders or files. Periodic online scanning is a good idea for those that run antivirus applications on their computers because those applications are frequently slow to catch threats. Because of these two approaches digital signature be scanned across the database but also across millions of computer and servers across the world.

REFERENCES

[1] Orbit-Computer Solutions.Com.

[2] www.google.com

[3] Network Security A Decision and Game-Theoretic Approach.

[4] Cryptography and Network Security By Atul Kahate.