NETWORK SECURITY AND NEXT-GENERATION FIREWALL(THIRD GENERATION)

Khan Uzma Shamim Ahmed [#1], Rane Mitesh [#2]
Master of Computer Application, IMCOST, Mumbai University, Mumbai, India.

Abstract— ***Nowadays* Network security is an important aspect in every field like government offices, Educational institute and any business organization. Network security is a challenging issue due to the complexity of underlying hardware, software, and network not independence between things as well as human and social factors. It involves decision making in multiple levels and multiple time scales and in multiple scenarios, given the limited resources available are malicious attackers and administrators defending network system. The resources be different from bandwidth, computing, and energy at the device level to manpower and schedule at the organizational level. Nowadays Data security is the extreme critical factor in ensuring the transmission of information via the network around the world. Threats to data privacy are most powerful tools in the hands of hackers that could use the vulnerabilities of a network to corrupt ,hack, demolish and steal the sensitive information. There are more network security measure to keep safe the data from attackers for example antivirus software, firewalls, cryptography etc. In this paper we study various types of attacks on network security and how to handle or prevent this attack, also studied that firewall work based on the port hoping so it break the security to overcome on this we see the application awareness Firewall.**

Keywords: **Virus, Firewall(Computing), security, attacks, Hardware Firewalls, Antivirus software ,Inspection.**

I. INTRODUCTION

Network security may have rules and regulations approve by a network administrator to avoid and checking unauthorized access, modification, harm, or denial of a computer network and network-accessible resources. Network security include the granting of access to data in a network, which is controlled by the network administrator. Users select or are allocated an ID and password or other credential information that allows them access to information and programs within their authority. There is a private and public computer network, that are used in everyday jobs conducting transactions and conversation among businesses, government agencies and individuals. Networks can be private, such as inside an organization, and others which might be open to public access. Network security ,Internet security is a tree branch of computer security typically related to the Internet, often including browser security but also network security on a more general level as it put to other applications or operating systems as a whole. Its objective is to establish policies and measures to apply 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 many times in the form of harmful which enter into the device by themselves without any knowledge of the user and sometimes in the form of unauthorized user who got the access of computer system for the purpose of alteration of stored data, to take information or keep to keen eyes on user activity. some of the common forms of the Attacks are: computers virus, Spam pashing spyware ,Cracking ,Adware ,Hacking , etc .These threats are basically present due to the ignorance shown by the users, weak technology and bad design of the network .To save or secure data from such network viruses one of the network security measure is antivirus programmed. When keeping in mind 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 interface channel.

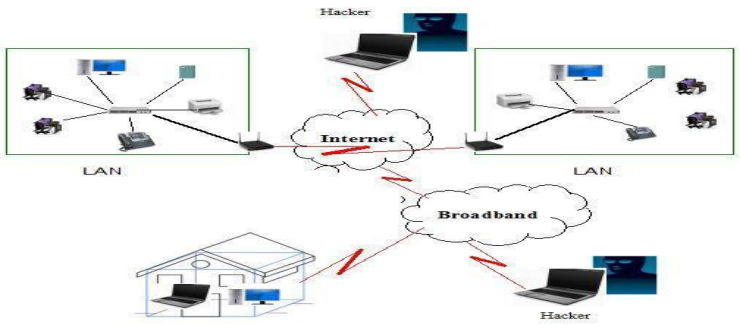


Fig 1. Malware protection Set up.

Virus: It is a program, script, or piece of code to cause damage, steal personal information, modify data, send e-mail, display messages, or some combination of these actions. when it executed, make a replica by inserting copies of itself (may be modified) into other computer programs, data files, or the boot sector of the hard drive; when this duplication succeeds, the affected areas are called "infected". Viruses often perform some type of harmful activity on system device, such as harming the system software by corrupting or destroying data, stealing hard disk space or Processing time, accessing private information ,displaying political or entertaining, comic messages on the user's screen, spamming their contacts, logging, or even rendering the computer is not useful. However, once the virus infects your computer, the virus can harm other computers on the same network. they can Stealing passwords or data, logging keystrokes, corrupting files, spamming your

email contacts etc. 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 operator or user. it can penetrate in a computer by various ways for example when one copy some data from the virus Infected system to different uninfected computer or it can be while downloading any given 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 helps to affect the operations of computers. 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 vulnerabilities increases, different terms have been introduced to specify the individuals involved. These terms are mentioned below

a. White hat- These are ethical hackers who looks for fragilities in networks and then reports these suspected files to the system owner so that they can be fixed. They are ethically opposed to the attack on computer systems. A white hat generally focuses on securing IT systems.

b. Hacker- This is a general term that is usually used to define a programming expert in computer. These are normally used in not so good way to define a professional that tries to gain access which is not authorized to network resources with malicious intent.

c. Black hat or Cracker- The exact opposite of White Hat hacker, Cracker is used to describe those professional who use their skill of computer based operating systems and programming skills to break and into systems or networks that they are unauthorized to access, this is usually done for personal or financial gain.

d. Phreak - This term is often used to describe a professional who manipulates the network, usually of phone in order to perform illegal activity. The phreaker breaks into the phone network, normally through a public phone, to make free long distance calls.

e. Spammer- This is often used to describe the person who broadcasts massage unsolicited e-mails. Spammers often use viruses to take control of any given computers and use them to send broadcast email messages.

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

III. Preventions:

1. Firewall:

Firewalls force to check 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(take from the identical military term of a combat limiting geographical feature). Firewalls works on the basis of source ip ,destination ip ,source port ,destination port they allow and reject the traffic. 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.

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

A firewall is a hardware or software that monitors the traffic flow through a network. Firewall can be configured to allow or denied traffic based on given criteria (ACLs). Firewalls allows or denies pings from a remote site to your computer or programs from your device that attempts to access remote computer without your knowledge.

Most of the windows software doesn't comes with inbuilt firewall. To view and windows firewall can be configure by below 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.

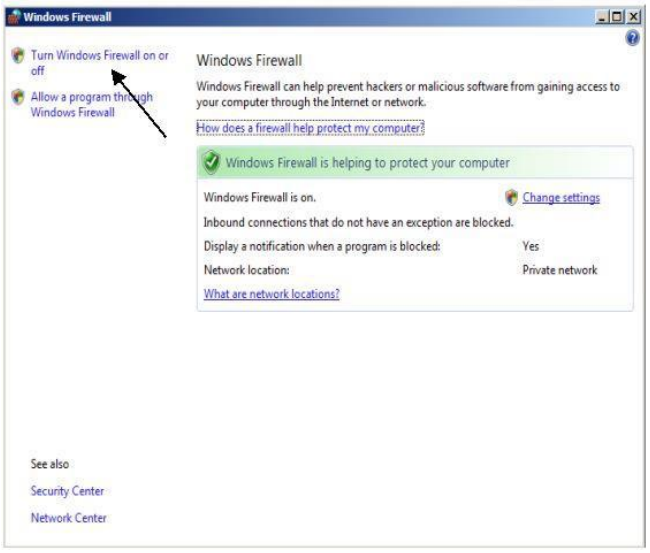
Click on start button

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



Click On
Click Apply
Then Click Ok

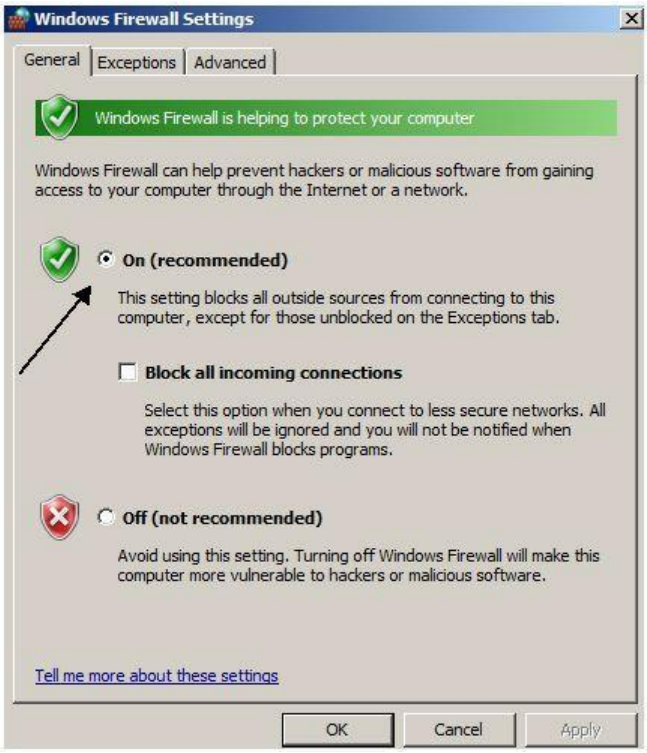


Fig.2.c. Successfully firewall applied

a. Network firewalls: It does not make any attempt to identify the virus based on TCP/IP ports, it directly blocks unauthorized programming from accessing resources .the system. Reports 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 request on certain TCP/IP ports. A firewall is designed to deal with broader system threats that usually come from network connections and penetrates into the system and is not an alternative to a virus protection system.

b. Hardware Firewalls:

Hardware-based firewalls protect all the devices in your network infrastructure. A hardware-based firewall is easy to administer and maintain than individual software firewalls. Hardware firewall integrated into a comprehensive security box. Additionally a firewall, the solution should consists of virtual private network (VPN) support, antispam , antivirus, antispyware, content filtering, and other security technologies.

II. Antivirus:

Antivirus and Internet security software can prevent a programmable device from intrusion by detecting and preventing viruses; Antivirus software was mainly shareware in early years of the Internet, but there are now various free security software on the Internet to choose from for various platforms .Antivirus software was basically invented 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 phishing attacks, online Privacy identity, online banking threats, social engineering techniques, botnets DDoS attacks, Advance Persistent Thread (APT). 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 developer test their current viruses on the famous anti-virus software to make sure that they are not identified before releasing them into the wild also one more reason is virus uses Graphics Processing Unit (GPU) to avoid identification from antivirus software. New viruses, particularly ransomware, use programming code to avoid identification by virus scanners. This type of ransomware virusarrives 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 basic principle; they can scan a file and then matches, its digital signature against the known intrusion. If the signature is matched in the database it reports, delete it or even disinfect it depending on the clients setting. This system however has a huge drawback, whenever a new malware found ;it takes time before the antivirus DB can be updated and during this interval the intrusion can already take complete control of the system, disables the antivirus or even hides itself from the antivirus. To limit this antivirus developers introduced a new system called online scanning and cloud antivirus. Cloud antivirus is a technology that uses lightweight agent software for intrusion detection on the secured device, while offloading the most of data analysis

to the provider's IT infrastructure. To implementing cloudAV includes scanning cautious files using multiple antivirus engines which was an early implementation of the cloudAV concept called CloudAV. Cloud AntiVirus was developed to send programs to a network cloud where multiple antivirus and behavioural detection programs are used concurrently in order to improve identification rates. in the same time scanning files using potentially inappropriate antivirus scanners is possible by copy a virtual machine per identification engine and therefore eliminating any possible issues. CloudAV is a solution for effective virus scanning on computers that lack the computing power to perform scans themselves .In online scanning to maintain websites with free online scanning capability of the full computer, important areas only, local harddisks, folders/files. Periodic online scanning is very good idea for those who run antivirus software on their network because those software are frequently slow to catch threats. Because of these two approaches digital signature scanned across the database and also across millions of computer and servers across the world.

Behavior based approach –

Nowadays all the software and Hardware based firewalls, restricts or allows traffic based on Source IP, destination IP, source port, Destination port.
There are multiple applications available nowadays which works on port hopping. That is these applications change their destination port and can be easily penetrate in any given network.
Applications like Skype, bit torrent works on port hopping which cannot be easily restricted by using traditional firewalls. So the firewall should be self-efficient to understand the behavior of traffic, for example – traffic consisting of voice, video or chat, so that the respective traffics coming from any source or destination can be restricted depending on their behavior.

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.

[5] Network Security Essentials, William Stallings, Prentice-Hall, 2000

[6] Security Technologies for the world wide web , Rolf Oppliger, Artech House, 2000

First Author Khan Uzma Shamim Ahmed student of 3rd year MCA.

Second Author Rane Mitesh student of 3rd year MCA