International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

A New Approach- Network Security

Nisha Trisal
(nishatrisal@yahoo.in)
(Student, Department of Elect.& Comm. Engg.
Dronacharya College of Engg. Gurgaon, Haryana)

Shivam Thakur
(shivamthakur83@gmail.com)
(Student, Department of Elect.& Comm. Engg.
DronacharyaCollege of Engg. Gurgaon, Haryana)

SumanPawar
(sumanpawar27@gmail.com)
(Student, Department of Elect.& Comm. Engg.
Dronacharya College of Engg. Gurgaon, Haryana)

(1) ABSTRACT

One of the most important part to personal computer users is network security. Security has become a topic of importance by the expansion of internet. Whenever we research about something we must know about how it evolved, so we have discussed over that issue also. Knowing the attack methods,allows for the right security to emerge. Many businesses shelter themselves by the means of firewalls and encryption mechanisms. The businesses form an INTRANET to remain linked to the internet but secured from possible threats. The architecture of the internet when modified can shrink the possible attacks that can be sent across the network. The research paper is an overview about the various incidents that have occurred in internet's lifetime. It has discussed about the various technologies that have been developed so far to prevent the network security. Apart from this it has also thrown light over the secure methods which an organization or an individual can take on for the security of their essential data. The entire field of network security is immense and in an evolutionary stage. The range of study encompasses a brief history dating back to internet early stages and the existing technologies used to overcome network security. In order to understand the research being performed today, knowledge of the internet , attack methods through the internet, and security knowledge is important and therefore they reviewed.

KEYWORDS:-internet protocol; encryption; e-commerce; password; cryptography

(2) INTRODUCTION

The world is becoming more interconnected with the arrival of the new internet networking technology.There is huge amount of private, commercial, military, and government information on network infrastructures wide-reaching. Network

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

security is becoming of great significance because of intellectual property that can be acquired on internet.

Fundamentally two different and synchronous network are available on internet. The internet is considered a data network. Since the current data networkconsists of computer-based routers, information can be obtained by unique programs. The synchronous networkwhich instead of buffer data consist of switches and therefore are not threatened by attackers. This is the reason behind security is emphasized in data networks, such as the internet , and it's links.

3) HISTORY

Elucidating our history once again when Arpanet was revealed, very little of it was designed or implemented with declaration and security as the main concern. On those times attackers or the hackers were not that intelligent that they could disrupt the system. Internet protocols were not developed to secure themselves. Within the TCP/IP communication heap, security protocols are not implemented. This leaved internet unlock to attacks. The Arpanet took birth on1969 which initiated internet.

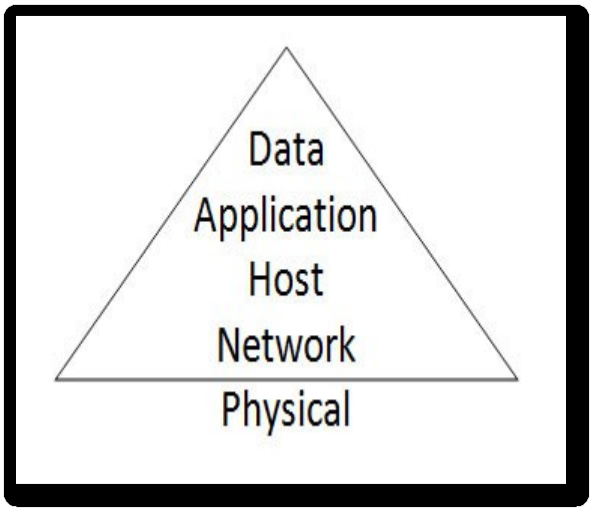
In 1980's an ordinary language for internet computers was found known as TCP/IP protocol. For the first time a free collection of networksprepared up the ARPANET nowviewed as internet. The internet was used by the corporations to be in touch with each other and with their customers.

In 1990s the internet became widespread and continued with the development ofmore browser for which NETSCAPE and MICROSOFT are in tough competition. Ever since then internet is rising on high peak and internet surfing has become equivalent to viewing TV for many users. Information securityunderway before the internet developed.For information security cryptographers developedanpuzzled machine to convert plain messages to encrypted text. A intelligent mathematician broke the code in 1930 which was later named as word "hacker" by some students in 1960's. Earlierinternet was limited to government contractors and academic researchers but it was Telnet protocol which made internet public.

The hacking and crimes regarding computers started to begin at that time. In 1986 an act was created because of LAN MURPHY'S crime of thieving information from military computers for computer fraud and abuse. A graduated student spread MORRIS WORMover 6000 susceptible computer connected to internet. Due to this CERT(computer emergency response team) was formed to aware computer users.

Subsequently security became a great concern as over 1000s of people surfed on internet at the same point of time. The security breaches can consequenceinto monetory losses to a greatamount. Investment in good security should be the primary priority for large organizations as well as for general users.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org



Approach to security.

4) WORST MOMENTS IN NETWORK SECURITY

As time does not remain the same, so not all days are just as good as than others when we come across the term network security.Here are some our picks for some of the pits in history.

i. Yahoo, Dell, , eBay,Amazon and CNN all once struck down by a massivespreading of denial-of-service attack because of a teen calling himself "MAFIABOY". He has beentrapped and sentenced to eight months of "open custody," anything that means, a light fine and limited use of the Internet.

ii. The "ILoveYou" worm scoots from Hong Kong around the world in seconds, affecting an expected 10% of all connected computers. It over flooded Inboxes of several organizations, counting the Pentagon and British Parliament which brought Business serversonto their knees.

iii. A neighbouring country to Russia named Estonia, of about 3 million people, had a powerful network infrastructure that came under a severecyberattack that made its central government, banking and media Web sites unavailable. Security experts examined the cyberattacksupposed that it was head out by the "Russian blogosphere," which triggered a second phase that incorporated specially designed bots, dropped onto home computers.

iv. Arpanet annoyed but presently we are with one and only internet.Digital Equipment Corp. marketing guy GARY THUERK got technical support to send what's measured as the first "spam" message to thousands on the government-funded Arpanet, predecessor of today's Internet. Arpanet management named the mass e-mail as a "flagrant violation" of Arpanet policy. Brilliant thing was they pinched that in the bud.

(a) Types of threads in Security

(i) PASSWORD CRACKING

It involves special types of vulnerabilities and decrypting techniques. Brute force attempt is the most popular form of cracking password . Brute force attack is a way of cracking an individual's username and password for a particular website by scanning thousands of familiar terms, words and names until a mixture of them is given to the server.

(ii)DENIAL OF SERVICE ATTACKS

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

These generallyoverwork a server andturn them intoworthless. The server is frequently asked to perform tasks that have need ofusing a large amount of resources until it can no longer function correctly.

(iii) SERVER USER EXPLOITS

It allows attackers to gain power of a system as if they were an administrator. They time and again use scripts to manipulate a database or a buffer overflow attack that cripples a system.

(iv)TORJANS

The software is considered to be the most unsafe in terms of E-Commerce security due to its capacity to connect behind closed doors and send confidential information. These are the special programs developed for specific purposes of communicating without the option of detection.

(v)IP SPOOFING ATTACKS

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to getway in to other computers. The identificationof the intruder is invisible by different means making detection and prevention complex.

5) TECHNOLOGIES DEVELOPED FOR NETWORK SECURITY

It is obvious that when something is made free it's security decreases. Since internet contains and communicates with data so threats will always remain a foremost concern. To avoiduseless access, defense and detection mechanisms were developed. Web developers and security professionals must apply and make use of effective security techniques and policies. Technology management must pursue the three R's of security – recognize, resist, and recover.

(i) CRYPTOGRAPHIC SYSTEMS

It prevents the data from being misused via converting the data into codes and ciphers into an insignificant data. Encryption and decryption occurs at receiver and server end only.

(ii) FIREWALL

The purpose of firewall is to sort out communications that may be ominous to a system. It restricts traffic to a system and allows pre-determined activity to go through filter. It is a usual border control mechanism or perimeter protection. The intention of a firewall is to obstruct traffic externally, but it could also be used to block traffic within. A firewall is the forefrontdefence mechanismin opposition to intruders. It is a system designed to avoid unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software , or a permutation of both[5].

(iii) INRUSION DETECTION SYSTEMS

An intrusion detection system (IDS) is asupplementary protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to identify an attack. IDS products are used to

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

supervise connection in determining whether attacks are been launched. Some IDS systems just monitor and vigilant of an attack, whether others try to obstruct the attack.

(iv) EFFECTIVE PASSWORD POLICIES

Implementation of the password policies which are helped to weaken out a password cracker's whose usefulness is essential. Accounts intercepts should be locked out after a scheduled number of consecutive erroneous username and password combinations. The ensuranceis that users utilizing the brute force attack are not being able to repeatedly attempt the login combinations. The IP address of thoseare blacklisted on the web server. As Minimum password lengths and the maximum occurrences of exact character may be two of many ways to enhance security.

(6)STEPS TOWARDS A SAFE NETWORK

Security must not be treated as a annoyance. It is more than just averting or restraining what people do. A good security enables the industries to operate their workssafely and securly by shielding revenue and profits that could be lost through data. The most essential part of your bull is treat security.The effort regarding the serious offenses which are against computer networks.

1. There must be an organization of laws which should agreement with state party and adopt a completediagnism of national laws which either will punish the serious crimes against the computerdiagnism of national laws which either will punish the serious crimes against the computer security network. The working of these laws are different in different countries as a relsult of malicious behaviour specify as offences within the country. Such inacted would be an admission to the aggrement as the necessary condition.

2. The state rebelives are the set of near universal which is basically a global problem.The near universal participation makes a problem globally.Each and every countries which is either connected to the internet or is a global network is a part of hazard and the exposure problem there must be an effort which will try to make a solotion to this.

(7)CONCLUSIONS

Network security is asignificant field that is ever more gaining interest as the internet expands. The security threats and internet protocol were examined to resolve the required security technology. The security technology is mostly software based, but many frequent hardware device are used. The present development in network security is not very notable. Initially it was understood that with the significance of the network security field, new approaches to security, both hardware and software, would be intensely researched. It was shocking to see most of the development taking place in the same technologies being currently worn. Collective use of IPV6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will confirm

efficient in guarding intellectual property for the near future. The network security field may have to develop more rapidly to deal with the threats further in the future.

8) REFRENCES

[1] Stallings, William. *Network and Internetwork Security: Principles and Practice*. Englewood Cliffs, NJ: Prentice Hall, 1995.

[2] Amoroso, Edward. *Fundamentals of Computer Security Technology*. Englewood Cliffs, NJ: Prentice-Hall, 1994.

[3] Brunner, John. *Shockwave Rider*. New York, NY: A Del Ray Book, published by Ballantine, 1975.

[4] Carroll, John M. *Computer Security*. 2nd edition, Stoneham, MA: Butterworth Publishers, 1987.

[5]Bellovin, Steve and Cheswick, Bill. *Firewalls and Internet Security*. Reading, MA: Addison-Wesley, 1994.

[6] Liu, Cricket, Jerry Peek, Russ Jones, Bryan Buus, and Adrian Nye. *Managing Internet Information Services,* Sebastopol, CA: O'Reilly & Associates, 1994.