International Journal of Management, IT & Engineering
Vol. 8 Issue 4, April 2018, ISSN: 2249-0558
Impact Factor: 7.119Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A Study on Cyber-Attack and Cyber Security

Suneetha
Assistant Professor,
DoS in Computer Science,
Karnataka State Open University,
Mysore-570006

Abstract:Presently, all the social, economical, commercial, cultural and governmental activities are carried out online. Money transactions and vital documents are shared online. Hence security plays a vital role to secure websites and all the information shared online along with e-payments done for e-commerce should be kept secured.Here we are studying a variety of cyber-attacks and different security methods. This paper explores how cybercrime has become a serious threat in our lives and we are going to look at a few of the different security methods that are being used to overcome cyber-attacks.

Key Words: cyber attack, cyber security, virus, antivirus, firewall,encryption

INTRODUCTION:

Today Internet is the fastest growing infrastructure in everyday life. Today we are able to send and receive any form of data like e-mail, audio or video just by the click of a button. Within a fraction of a second, we can connect the whole world through information but how far our data, information are secured in internet is not bothered by the people.Through cyber security, we can secure our data. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cybercrimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding an individual their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cybercrime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber-crimes.

The purpose of cyber-attacks is an attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systemand harm companies financially. In some other cases, cyber-attacks can have military or political purposes. Cyber security follows real-time information on the latest IT data. So far, various methods hadbeen proposed by researchers around the world to prevent cyber-attacks or reduce the damage causedby them. The aimof this study is to survey the various types of cyber-attacks and security measures.

The most important cyber-attacks methods are Denial of service,logical bomb, Abuse tools, Sniffer, Trojan horse, Virus, Worm,Send spam, and Botnet.

VIRUS

It is the type of malicious software that, when executed replicates itself by modifying other computer programs.

Computer viruses causes economic damage due to system failure, corrupting data, increasing maintenance cost etc.

WORMS

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computer. Many worms are designed only to spread, and do not attempt to change the systems they pass through.

TROJAN HORSE

commonly known as a Trojan , is a name for malicious software that tends to be harmless, so that a user by will allows it to be downloaded onto the computer. Trojan allow an attacker to hack users' personal information such as banking information, email passwords, personal identity. It also affects other devices connected to the network.

MALWARE

MALWARE is a term short for malicious software, used to destroy computer operation, gather very sensitive

information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term malware is sometimes used for bad malware and unintentionally harmful software.

In the Denial of service method, the authorized users' access to the system and vice versa is lost. In fact, theattacker from one point starts immersing the target computers in various messages and blocking the legal flow of data. This prevents any system from using the Internet or communicating with other systems.

Sniffer is also a program that eavesdrops on routed information and looks for specific information such as passwords by examining each packet in the data stream

Abuse tools are available to the public that can detect and enter vulnerabilities in networks with different skill levels.

A logic bomb is another type of attack in which a programmer enters code into a program in which, in the event of a specific event, the program automatically performs a destructive activity.

Botnet is a network of infected remote control systems, which is used to distribute malware, coordinate attacks, and spam and steal messages.

CYBER SECURITY

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take of all the required security measures.

FIREWALL

A computer firewall controls the access between the networks. It contains filters depending upon one firewall orthe other. Firewall is basically a computer security system that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

ANTIVIRUS

Antivirus software and internet security programs are able to project a programmable device from attack by detecting and eliminating the viruses. Antivirus software was used in the early years of internet but now with the development several free security applications are available on internet.

Encryption

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information.

CONCLUSION

In this paper we have summarized about the various cyberattacks and the various security methods that can used to prevent our device from getting attacked.

References:

1. https://en.wikipedia.org/wiki/malware
2. https://en.wikipedia.org/wiki/virus
3. https://en.wikipedia.org/wiki/botnet
4. https://en.wikipedia.org/wiki/firewall
5. Saloni Khurana , A Review Paper on Cyber Security, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181,VIMPACT - 2017 Conference Proceedings,Volume 5, Issue 23

6. Nikhita Reddy Gade, Ugander G J Reddy, A Study Of Cyber Security Challenges and Its Emerging Trends On Latest Technologies,February 2014,https://www.researchgate.net/publication/260126665.