International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228379

Cyber Security Issues and Challenges - A Review

Amit Kumar
Assistant Professor, Department of Computer Science & Engineering, Maulana Azad College of Engineering & Technology, Patna, Bihar, India

Article Info
Volume 8, Issue 3
Page Number : 269-273

Publication Issue :
May-June-2022

Article History
Accepted: 01 June 2022
Published: 07 June 2022

ABSTRACT

Cyber security has become essential for information security. Keeping the information safe is one of the major challenges nowadays. Given the unrestricted number of free websites, the Internet has undeniably opened a new way of exploitation known as cybercrime. Governments and private sectors are taking many measures in order to control these cybercrimes. Handling cyber security is still a very huge concern. This research paper focuses on the various problems in cyber security during the current scenario .It also bring on focus on emerging technologies in the field of cyber security , ethics and the trends changing the features of cyber security.

Keywords : Cyber Security, Cyber Crime, Cyber Ethics

I. INTRODUCTION

Almost everyone is aware of the phenomenal growth of the Internet. Data communication is playing a major role in today's human life through sending and receiving any form of data like text, image, video or audio files just by click the button but that person don't know whether that message transmitted or sent to the other person safely without any leakage of information. In today's technical environment many recent technologies are belonging to the fast growth of internet technology. But according to these emerging technologies are unable to prevent the private information in a very effective way and hence these days cyber crimes are increasing day by day. Recently, more than 60 percent of total commercial transactions are done through online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue in the IT sector. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. The latest technologies like cloud computing, green computing, mobile computing, E-commerce, net banking are required high level of information security.

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based

variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent. Cyber security is a term of security which is implicated through diversified disciplines, most of them focusing on technical or psychological problems such as computer science, criminology, economics, engineering, information systems, management, medicare, neurophysiology, psychology, sociology, etc. It afford the people with discussions about behaviours and motivations, benefits and consequences about cyber crime and security.

Cyber security is one of the information system management by individuals or organizations to direct end-users security behaviours, on the basis of personal perceived behaviours toward potential security breach in work and non-work environment. The extant study of cyber security explores three main streams: individual behaviours toward information security in non-work setting, employee behaviours toward information security in work setting, and organization information system security policy (ISSP) compliance and the related issues.

II. Kinds of Cyber Attacks

Following are the types of Cyber attacks observed:

Denial of Service Attacks(DOS)

The most common sort of Denial of Service attack involves flooding the target resource with external communication requests.This overload prevents the resource from responding to legitimate traffic, or slows its response therefore considerably that it's rendered effectively out of stock. Resources targeted during a DoS attack are often a particular laptop, a port or service on the targeted system, a complete network, a part of a given network any system part. DoS attacks might also target human-system communications, or human-response systems. DoS attacks may target tangible system resources, like process resources; configuration info; state information. Moreover, a DoS attack are often designed to: execute malware that maxes out the processor, preventing usage; trigger errors in machine computer code or sequencing of directions, forcing the pc into associate degree unstable state; exploit software package vulnerabilities to sap system resources; crash the software package altogether. The preponderating similarity in these examples is that, as a results of the in Denial of Service attack, the system in question doesn't respond as before, and repair is either denied or severely restricted.

1) Remote to Local Attacks

A remote to local (R2L) attack is a kind of attack where an attacker send packets to a machine over networks, then exploits the machine's vulnerability to illegitimately increase local access to a machine. It happens when an attacker who has the capability to send packets to a machine over a network but who does not have an account on that machine develops some vulnerability to achieve local access as a user of that machine.

TCP ACK flood

In this attack, lots of protocol ACK packets are sent to victim to utilize its system and network resources. Looking on the OS, AN open port or closed port would possibly reply a protocol RESET packet, inflicting a lot of traffics and employment on the victim and victim's network. AN evolution of this attack consists in flooding the victim with protocol ACK packets with spoofed supply information processing, random sequence range and random port range within the packet.

2) Signature based Approach

Signature based approach of mishandling discovery works just comparable to the existing anti-virus software. In this approach the semantic description of an attack is analyzed and details is used to structure

attack signatures. The attack signatures are structured in such a way that they can be searched using information in audit data logs produced by computer systems.

Protocol Flooding

Probably, whenever we've detected regarding protocol flooding attacks, we tend to were talking a few protocol SYN flood attack. However, it's potential to expertise a protocol flooding attack that's not taking advantage of the protocol multilateral handshaking. It's additionally potential to act a protocol flooding attack taking advantage of different TCP's finite state or TCP's flags.

Ping of Death

The TCP/IP specification permits for a most packet size of up to 65536 octets (1 computer memory unit = eight bits of data), containing a minimum of twenty bytes of science header data and zero or a lot of bytes of elective data, with the remainder of the packet being information. It's famous that some systems can react in hit and miss fashion once receiving outsized science packets. In specific, some reports indicate that web management Message Protocol (ICMP) packets issued via the "ping" command are accustomed trigger this behavior. The "ping" command is accustomed construct outsized ICMP datagram's (which square measure encapsulated among associate degree science packet), taking advantage that several ping implementations by default send ICMP datagram's consisting solely of the eight bytes of ICMP header data, however enable the user to specify a bigger packet size if desired. An offender sends associate degree ICMP ECHO request packet that's abundant larger than the utmost science packet size to victim. Since the received ICMP echo request packet is larger than the traditional science packet size, the victim cannot assemble the packets. The OS is also crashed or rebooted as a result. The Ping of Death could be a typical TCP/IP implementation attack. During this assault, the DoS offender creates associate degree science packet that exceeds the science standard's most sixty five, 536-byte size. Once this huge packet arrives, it crashes systems that square measure employing a vulnerable TCP/IP stack. No trendy package or stack is prone to the straightforward Ping of Death, however however it had been a long-standing drawback with OS systems.

Teardrop

The Teardrop, though, is associate degree previous attack that depends on poor TCP/IP implementation that's still around. It works by busy with however stacks assemble science packet fragments. The trick here is that as science packet square measure generally shifting into smaller chunks, every fragment still has the initial science packet's header, and field that tell the TCP/IP stack what bytes it contains. Once it works right, this data is employed to place the packet back along once more. What happens with Teardrop although is that our stack is buried with science fragments that have overlapping fields. Once the stack tries to assemble them, it cannot bed, and if it doesn't grasp to toss these trash packet fragments out, it will quickly fail. Most systems shrewdness to take care of Teardrops currently and a firewall will block Teardrop packets reciprocally for slightly a lot of latency on network connections since this makes it disregard all broken packets. Of course, if we have a tendency to throw a lot of Teardrop busted packets at a system, it will still crash. Several different variants like Targa, SynDrop, Boink, Nestea Bonk, TearDrop2 and NewTear square measure on the market to accomplish this type of attack.

Land

A LAND attack consists of a stream of transmission control protocol SYN packets that have the supply science address and transmission control protocol port range set to an equivalent price because the destination address and port range (i.e., that of the attacked host). Some implementations of TCP/IP cannot handle this in theory not possible condition, inflicting the package to travel into a loop because it tries to resolve perennial connections to itself. Service suppliers will block LAND attacks that originate

behind aggregation points by putting in filters on the ingress ports of their edge routers to see the supply science addresses of all incoming packets. If the address is among the vary of publicized prefixes, the packet is forwarded; otherwise it's born.

Echo/Chargen

The character generator (chargen) service is intended to easily generate a stream of characters. It's primarily used for testing functions. Remote users/intruders will abuse this service by exhausting system resources. Spoofed network sessions that seem to come back from that local system's echo service can be pointed at the chargen service to form a "loop." This session will cause huge amounts of data to be passed in an endless loop that causes heavy load to the system. When this spoofed session is pointed at a remote system's echo service, this denial of service attack will cause heavy network traffic/overhead that considerably slows down the network. It should be noted that an attacker does not need to be on our subnet to perform this attack as he/she can forge the source addresses to these services with relative ease.

Naptha Attack

The number and kind of resources that associate wrongdoer will target for a denial-of-service attack square measure several and varied. The Naptha work highlights a collection of them that some specific defenses exist. In general, any system that enables important resources to be consumed while not certain is subsubject to denial-of-service attacks. Naptha and similar network attacks square measure additional dangerous for many reasons: They can be done "asymmetrically" – that's, the wrongdoer will consume huge amounts of a victim's restricted resource while not equal resource expenditure. In combination with alternative vulnerabilities or weaknesses, they'll be done anonymously. They can be enclosed in distributed denial-of-service tools.

Cyber Ethics

Cyber ethics are nothing but the code of the internet. Practicing cyber ethics are good chances to use the internet in a correct and protected way. The below are a few cyber ethics one must follow while using the internet.

Ethics 1: To communicate and interact people with each other with the assistant of internet. Instant messages and email make it contact to stay in connect with the family members and friends, share knowledge and information with people among the country with the specific organization and all around the world.

Ethics 2: Internet is measured as world's leading library with information on all the topic in any specific subject area, hence using this information in a proper and legal way is always essential.

Ethics 3: People are not able to operate other persons mail account with their passwords.

Ethics 4: On no account try to send any kind of malware to other's systems and make them fraudulentand damage.

Ethics 5: Do not share the personal details to anyone as there is a good opportunity of other persons mishandling the mail account and finally that person must be in a problem.

Ethics 6: When the person is in online do not pretend to the other person and never try to make any fake account on some other people as it would become a trouble.

III. CONCLUSION

The new world of information society with global networks and cyberspace will inevitably generate a wide variety of social, political, and ethical problems. Many problems related to human relationships and the community become apparent, when most human activities are carried on in cyberspace.Some basic ethical issues on the use of IT on global networks consist of personal privacy, data access rights, and harmful actions on the Internet. These basic issues have been solved partially using technological approaches, such as encryption technique, SSL, digital IDs and computer firewalls. Besides these protection technologies, legal laws are also needed in cyberspace

to address hundreds of countries, which are incorporated into one global network. Guidelines and strategies should be implemented so that global information can be exploited in a socially and ethically sensitive way for our future benefit and applications. Cyber security is a vast issue that is becoming more essential because the world is becoming extremely interconnected, with networks being used to carry out critical transactions.Everyone has a different idea regarding security policies and levels of risks. The key for building a secure network is to define what security need of the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. Hence it plays a vital role in information security.

IV. REFERENCES

[1]. A. Sternstein, “Pentagon Disconnects iPhone, Android Security Service, Forcing a Return to BlackBerry for Some,” Presented at NextGov, Dec. 3, 2013.

[2]. International Telecommunication Union (ITU), “Global Cybersecurity Index (GCI) 2017,2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[3]. Chang, L. Y. C. (2012). Cybercrime in the Greater China Region: Regulatory responses and crime prevention across the Taiwan Strait. Cheltenham: Edward Elgar Publishing.

[4]. Etter,B. (2001), The forensic challenges of E-Crime, Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide.

[5]. Etter B. (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand.

[6]. Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer crime Laws, Santa Clara University, Vol 16, Number 2.

[7]. Seamus O Clardhuanin , An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Summer 2004, Vol 3, Issue 1. 2004.

[8]. Farmer, Dan. & Charles, Mann C. Surveillance nation. Technology Review; Vol. 106, No. 4, 2003: Pp. 46.

[9]. Harrison, A. Privacy group critical of release of carnivore data. Computerworld; Vol. 34, No. 41, 2006: Pp. 24.

Cite this article as :

Amit Kumar , "Cyber Security Issues and Challenges - A Review", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 3, pp. 269-273, May-June 2022.
Available at doi : https://doi.org/10.32628/CSEIT228379
Journal URL : https://ijsrcseit.com/CSEIT228379