ISBN: 978-93-92995-10-1

CYBER HACKING

HARSHITH REDDY PARREDDY

VARSHITH REDDY VUYYURU

RAM SAI MANYALA
Email ID: harshithreddyparreddy@gmail.com

Abstract
Living in a world where the technology is booming the world, where there is no need to worry for the present or the future and has many advantages compared to the past decades, it has also given people the power to use it for the right as well as the wrong. The wrong has also been increasing drastically over the period of time. They are the hackers who try to exploit the cyber network constantly and degrade the trust that the legitimate user have no the advancement in it and the dependency is deteriorating drastically.
Keywords: *hacking, illegal access, cyber crime, protection, awareness*

Introdution

Hacking means steeling of personal data in an unethical way without the knowledge of the individual. Hacking refers to identifying the weakness of the computer. It also allows to access the personal data which is secured. It also refers to modifying the computer software and hardware to complete a goal that an "individual requires". Those individuals who require the personal data of an individual or an organisation are known as "hackers".

Hacking is considered to be both a boon and bane to the society. Ethical hacking is a boon for the society .Ethical hacking means identifying the weakness of the computer and to upgrade the weakness of the computer. There is other kind of hacking known as unethical hacking which is a bane for the society. Unethical hacking means to known the personal data of a particular individual or organisation without the knowledge of the user.

Literary Review

[1] Cyber terrorism is one of the major problems which the world is facing as there is advancement in technology and use of it. It has many reasons for it to be one of the most opted and learnt among people. Few are for money, power, fame and to access information. The millennium bug has become an increasing threat to the organizations who lose all their originality. Hackers may also target individuals or groups to obtain what is desired by them.

[2] Over the past decades there has developed more problem on cyber terrorism. Much before there had been great about the cyber terrorism, including stated fear about their computer that about the hacking. The fear become more by the problem often referred to as the millennium bug by those to dramatize the threat. Despite the fat that these fears have yet to got matched with real fears and real event, in reality when we take the issue of terrorism the danger of cyber terrorism is always is on the top of the list of the social fears. From this there will be large number of deaths and lot of damage to the nation. That same is true for the cyber terrorism. However, there is a little concrete of the terrorism preparing to use the computer as a tool for harming the people. This may hurt the people and public. The hacker orders the person to do illegal things so that the hacker will be happy.

[3] This paper gives us information about the various awareness programmes and defensive methods practiced or taught to people for better knowledge about the network security and the precautions to be taken when and if you are caught up in any such situation. There are also various competitions held such as cyber defense competitions which helped them understand the situation better and also spread this to many more institutions for the betterment of the world to face a positive cyber environment.

[4]Cyber physical system is a organisation which aims at regulating the physical environment in which people work. There are many steps and challenges faced by the CPS in maintaining a better cyber world. Few of them are monitoring the exchange of various information, integrating with other organisations for better security, providing authenticity, checking on denial of service attacks which are the most frequent of all the issues which is done just for fun also. Even snooping and eavesdropping ,which are the basic of all the issues, come under network security. These organisations face a lot of challenges in their work of maintaining a secure environment for its legitimate users and have developed a framework to ensure the same**.**

[5]This paper talks about the various cyber crimes done by people using unlawful acts where the computer is a tool or a target or used as both. Some of them are cyber stalking, spoofing, gambling, snooping into other peoples emails, personal accounts and installing trojan horses onto pc's of other people to continue the process. It also discusses the preventive methods which are to be taken like using firewalls, antivirus softwares, etc. There are also methods to detect the intrusions which are discussed in the paper. It also mentions the work of the Cyber law of India which was passed in the year 2000 and their response to the crimes being carried out.

[6]Now a days there is much more importance for the data they have in the companies. The data which they have can be used in ethical way as well as in the unethical way. If everyone is ethical then there will be more job opportunities in any field. In the most of the companies there are more requirements for the job that deals with the data protection. Giving security for the data is a relatively a lastest development that requires each and everybody involved to make it work.in those companies many of the information professionals use their skills to protect the data what they have. Hacking is usally done to steal the data of any company or an organization and make an advantage of it and earn money of it. Some of the professionals use this data in unethical way to avoid the payments for the required services .this is not only unethical but also it is a crime and it is banned in many of the countries.

[7] The security to be provided mainly focuses on the availability, integrity and confidentiality of the information of its users. It tracks its illegal users by using the TCP/IP protocol where the IP address is used for back tracking and it allows the incharge people to get the person who has been involved in such activities. Damage caused due to such practices leads to huge loss for the huge multinational companies , damage to their reputation and many more. The problem may also be because of the use of poor secured code and the carelessness of the company or the organisation undergoing the loss.

[8]Cyber attacking has been increasing in a fast rate where they disrupt the normal functioning of the network due to malicious network events and other intensions such as the greed for money, acquiring of the information of others illegally. Some of them create user-friendly softwares which get directly downloaded on to the desktop directly and do the backend server upload work, just like trojan horses and corrupt the other files and softwares on the same MAC address also which leads to the total control in the hands of the attackers.

[9]Cyber hacking is palying now a dominated role in the society.even a small thing that was done using technology can be known by this cyber hacking.we are watching different situations everyday in megacities like Hyderabad Mumbai Delhi Chennai etc . The police making efforts to stop cyber hacking and they are even reducing it but not in a large scale . Recently in Hyderabad situation took place with the help of Cyber hacking the hacked server of a big IT company stole the company data and sold it to other IT companies for huge amount. It took almost 15 to 20 days to catch that cyber hacker by the police. Like this many incidents are taking place in our day to day life and this server hacking is increasing day by day. The former President of America Barack Obama said that a company's economy depends on the cyber security of the country.

[10] This paper discusses about the various denial of service attacks such as denying the right to access the information, denial of access to applications by blocking the site, denial of access to a website by sending unwanted messages to it, denial of access to resources by not giving access to that person. The improvements which can be made are multiple network monitoring, connection state tracking, predicting source address, improving the infrastructure of the firewalls being used which enhances better security and doesn't allow any malpractices to happen.

[11]Many international terrorists gain knowledge about how to hack and gain illegal information and use it against the computers in the US especially. There are many ways of attack suck as physical attack, electronic attack and computer network attack. They lay a critical plan on how to get their tasks done and work as a team to get work done easier and in a better way. These professionals also create a link between hackers and terrorists where they partner together and get things done at an even larger scale.

[12]Attribution is defined as identity of an attacker's intermediary.in normal words it is know as "source tracking" instead we call it as "attribution", and in commercial world it is distributed denial of service(DDoS)attacks. It means intermediates but not only attackers. A resulting identity may be a persons name, an account, or simply information about the person who is operating the hacking things

Findings

We found that hacking has been used for both ethical and unethical practices and the good about it is that there is awareness also being spread to change the world of cyber networking and the bad is that they try to gain unwanted access to information of others which puts them in huge loss and may also lead to closure of the organisation.[13] "Searching becomes complex depending on large volume of data that are usually in the form of unstructured data, searching similarity over large volume of data with less response time and retrieval accuracy".

Conclusion

There can be better and stronger usage of coding and backup used when various softwares are launched and continuous check on the exchange of information in each and every part of the world. Also the punishments for such illegal practices should be made more stringent, thus expecting a reduction in such problems thereafter.

References

Anderson, R. S. (2009). *Cyber security and resilient systems*(No. INL/CON-09-16096). Idaho National Laboratory (INL).

Anderson, R. S. (2009). *Cyber security and resilient systems*(No. INL/CON-09-16096). Idaho National Laboratory (INL).

Conklin, A. (2006, January). Cyber defense competitions and information security education: An active learning solution for a capstone course. In *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on* (Vol. 9, pp. 220b-220b). IEEE.

Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium?. *Computers & Security*, *18*(1), 28-34.

Jain, N., & Jain, K. (2011). Cyber Crime: Prevention, Detection and Prosecution. In *First International Conference of the South Asian Society of Criminology and Victimology (SASCV), 15-17 January 2011, Jaipur, Rajasthan, India: SASCV 2011 Conference Proceedings* (p. 116). K. Jaishankar.

Schuba, C. L., Krsul, I. V., Kuhn, M. G., Spafford, E. H., Sundaram, A., & Zamboni, D. (1997, May). Analysis of a denial of service attack on TCP. In *Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on* (pp. 208-223). IEEE.

ShanmugaSundari, P., Subaji, M., & Karthikeyan, J. (2017). A survey on effective similarity search models and techniques for big data processing in healthcare system. *Research Journal of Pharmacy and Technology*, *10*(8), 2677-2684.

Stohl, M. (2006). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?. *Crime, law and social change*, *46*(4-5), 223-238.

Sukhai, N. B. (2004, October). Hacking and cybercrime. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 128-132). ACM.

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *IJ Network Security*, *15*(5), 390-396.

Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C. K., & Chow, K. P. (2010, December). Security issues and challenges for cyber physical system. In *Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom)* (pp. 733-738). IEEE.

Wheeler, D. A., & Larsen, G. N. (2003). Techniques for cyber attack attribution (No. IDA-P-3792). INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA.

Wilson, C. (2003). Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress. *Focus on Terrorism*, *9*, 1-42.