International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Network Security and Ethical Hacking

Anjali V Prajapati[1], Vikram Patalbansi[2]

[1]Student of Department of MCA, Late Bhausaheb Hiray Samiti Trust, Hiray Group of Institutes

[2]Mentor and Professor

Abstract: ***Networking enabled us to be connected to each other and devices thereby making it easy to interact with devices and people but it also can be used into compromising the privacy of its user and of the people connected to it. Network security is one of the major aspect to be considered also it is one of the most invested factor in an organization. With introduction of new technologies like internet of things, AI etc. besides making our life easier can also result in compromising it if not monitored and protected in a proper manner.***

Keywords: Networking; Ethical hacking; Internet of things (IOT); Artificial intelligence; Network security; Computer network; SS7; Privacy concerns

1. Introduction

Network Security and Ethical Hacking is a small but important part of computer science. In this we talk about security of our networks either it is telecommunication network or any other one. When we talk about Ethical Hacking it shows a type of hacking in which we don't harm any individual, any organization or any group. Networks plays a major role in our everyday lives including either talking over phone or connected through internet. With connectivity increasing day by day it is highly required that we consider our security and privacy at some point with all those unethical hackers eyes over our data it could be a catastrophe with all our information we have online. Damage a hacker can typically varies it can be financial loss, Encrypted files and demand for ransom or spying over a person or company without their knowledge. Cybercrime is increasing and cybercriminals are getting smarter ethical hackers are needed to prevent our systems from being compromised.

Techniques/Implementation

Networks form a major part of our day to day life. Most of our work includes networking no matter the place networks has enabled us to connect with each other people as well as devices thanks to IOT (Internet of Things) devices can be controlled remotely. Besides being able to connect cloud networks enabled us to be able to access the data from anywhere and anytime. However having so much of tech the state of privacy as well as network security is quite poor which results into our data being hacked or used for malicious purposes it is now no much difficult to fake ones identity. The solution to such a problem can be a term called ethical hacking.

Hacking in context of today's time is being defined as a crime or a criminal activity though it was not always so. Hacking is nothing but now the question is why and how the concept of hacking do came into existence? This happened because companies without testing their products wants to release their products into market which provides them profit but also with a compromised security of that product and if that product uses networking techniques it can also be manipulated to transmit other information and private data to the attacker thereby compromising the privacy. Network at present time is highly prone to many security issues so if a community of hackers to attack a certain system running any Operating System it's security flaw will be revealed thereby giving company who owns the product to provide an update for the software thereby fixing the flaws. Same technique can be used for applications also. However the process in terms of security will become much more efficient if the steps stated above are performed thoroughly before launching a certain software into the market which will obviously prevent the unauthorized access to a good percentage.

But the community responsible for testing may use the bugs or flaws so found to their own personal advantage. Now the question arises about how to prevent it? Though the person reporting the flaws discovered is rewarded with a certain gifts still the flaw can be maliciously used by some ill intentional people. In hurry of releasing the product into market the security is compromised. One solution to this problem may be such that if a developer wants to release its product into the market it will have to pass certain tests which will be conducted an organization or a committee which will work independently and the product will not be launched into the market until unless it is certified by that organization to be secure and now further tests and exploitation will be done publicly which will beside providing a tough challenge to the people trying to exploit flaws in the software will also provide a secure software or product to the general public. Another alternative for this can be doing the scanning task while development of the different components of software application, this can be done with the help of either a human or the objective can also be accomplished with the help of a software where certain definitions or instructions will be applied to the software to be tested which will expose it's vulnerability a technologically unsound or a slang word for breaking into a system though it is many times being used for personal profits, notorious activities. However, if seen deeply and searched it is just a tool and it purely depends upon the intentions of the person or a community using it.

Hacking may be in today's era of internet and digitization may be used for testing for certain issues and penetration techniques that a person or more precisely a cracker can apply to exploit a certain technology (may be a highly

complicated software, Application, Operating System or a Network) [1]. However the tool needs to be periodically updated. The tool can be effectively used for cyber forensics besides being used for software testing purposes.

As it is quite clear that the level of digital media as well as other fields in computer science like software development, networking, internet of things (IOT), Artificial Intelligence etc. is going to be on next level and with rise in development and digital revolution it is obvious that cybercrime will also encounter an increase and having such a tool like ethical hacking and it's experts will be quite necessary with increasing number of cybercriminals. Though it is a hypothetical concept but AI can actually be used in prevention of hacking and bypassing increasing a systems security. AI based on the previous hacks and flaws can be taught to prevent them by automatically implementing the necessary steps. Though it'll be a highly complicated task to do as it will be really tough to train it even smallest variations should be considered to prevent anyone from bypassing the system. Also the AI will need to be updated on the latest techniques and strategies for it to work as desired. With devices connected to the internet is increasing, the need for protecting them is also increasing.

Now the term hacking is not just limited to the field of computer science but has also been encountered into the field of electronics and its wide use can also be seen in IOT (Internet of Things). In the era of internet of things where many devices are connected to the internet thereby providing a better health care, comfortability, smart cities etc. the privacy concerns and security complications. Since IOT enabled our devices to be connected to the internet also provided a way to bypass them compromising the user security as well as privacy. Also, not to forget the fact that IOT and AI sort of goes hand in hand. Think of it as the body and brain just like a human body consist of sensors here the IOT devices will collect and provide the raw data and will feed it to the AI now at this point of time if an AI can be designed such that the security implementations can also be done for any kind of intrusion detection this will surely result in a better security thereby reducing the flaws. However designing such an AI will not be an easy task with all the knowledge of previous attacks and also the algorithm should be good enough to predict future vulnerabilities based on the previous data which already implies that the database of such an AI programmer should be large enough to achieve the above stated target With attacks like click jacking, DDoS (Distributed Denial of service), Malwares, Trojans, Keylogging it is highly desired that intrusion prevention is becoming highly important [2]. An automated system should be deployed which will be intelligent enough to take measures based on the attacks [3].

Setting up of rogue cell towers or IMSI catchers enabled exploiters to listen into our calls and text messages using a security flaw in SS7 (Signal System 7) [4]. The hackers can access anyone's cellphone through this anywhere in the world. This can be used to cashing out someone's bank account too. As operators migrate to IMS and LTE many value added services still uses the SS7 signalling protocol for text messages, payments etc. MAP (Mobile Application Protocol) uses SS7 network and besides IMS uses MAP which is used for voice messaging [4].

2. Conclusion

So the conclusion is this that we can use Artificial Intelligence to prevent hackers to access our network either it is a computer network or Internet of Things. In this process we need to taught AI that "How to prevent Hacker to bypass our network". Besides making our life comfortable networks can also be used to compromise it so, it depends upon how smartly and securely we use it because doesn't matter what it is nothing is unhackable.

References

[1] Smith B, Yurcik W, Doss D (2002) Ethical Hacking: The Security Justification Redux in Technology and Society.
[2] Utkarsh K (2013) System Security and Ethical Hacking. International Journal of Research in Engineering & Advanced Technology 1: 1-4.
[3] Joshi MR, Karkade RA (2015) Nerwork Security with Cryptography. IJCSMC 4: 201-204.
[4] Mobile Telecommunications Protocols for Data Networks by Anna Hac. University of Hawaii at Manoa, Honolulu, USA.