International Journal of Ingenious Research, Invention and Development
ISSN (Online): 2583 648X

Volume 1 | Issue 2 | February 2023
Scientific Journal Impact Factor (SJIF 2023) = 3.647
DOI: 10.5281/zenodo.7821165

ETHICAL HACKING

Dr Sachin Agrawal[1], Dhanashri Phuke[2]
[1]*Assistant Professor, CSE, College of Engineering and Technology, Akola, India*
[2]*Graduation Student (BE Final Year), CSE, College of Engineering and Technology, Akola, India*

Abstract: In the early 1900's if anyone would have said, that just in a few more years, all humans could carry a portable device in their pockets which will give them access to almost all details they were searching for any time of the day, then there might be a possibility even the simple thought would have been rejected and looked down by majority of people. But now we know that is altogether possible and how technology has made our day-to-day life easy. With just few clicks we can now see and talk to a person in almost different country or transfer money from one continent to the other. However, with ease of access for technology there are several threats, vulnerabilities which we cannot deny. These dark sides lead to the rise of unauthorized access and challenges on protecting our privacy which lead to the rise of unauthorized access and a new term was born Hacking. The research area of this project is about understanding the world of Hacking. The purpose to choose the topic of ethical hacking is because in the coming years, almost all things will be converted into either digitalize world or will be automated, and as our life's will be more depended on the technology, we need to understand the pros and cons for the same. The basic methodology used for completing this project was interacting with the ethical hackers and internet searches. The research helped me to draw result to understand how intentions are what make a hacker/s categorized in different types, which can help society or can even destroy the society.

Keywords: Network Security, Data Security, Hacking, Cracking, Ethical Hacking, etc.

I. INTRODUCTION

The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As with most technological advances, there is also a dark side: **criminal hackers**. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. With these concerns and others, the ethical hacker can help.

II. SECURITY

Security is the condition of being protected against danger or loss. In the general sense, security is a concept like safety. In the case of networks, the security is also called the information security. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Usually, the security is described in terms of CIA triads. The CIA are the basic principles of security in which "C" denotes the Confidentiality, "I" represents Integrity and the letter "A" represents the Availability.

International Journal of Ingenious Research, Invention and Development
ISSN (Online): 2583 648X

Volume 1 | Issue 2 | February 2023
Scientific Journal Impact Factor (SJIF 2023) = 3.647
DOI: 10.5281/zenodo.7821165

2.1) Integrity:

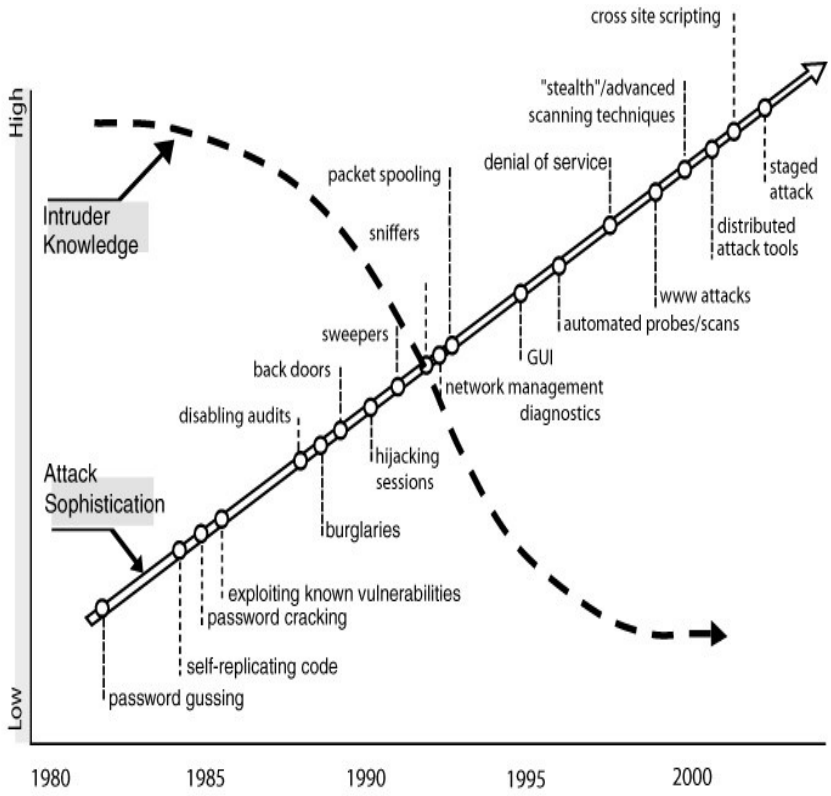
Integrity means that data cannot be modified without authorization. This means that the data seen by the authorized persons should be correct or the data should maintain the property of integrity. With out that integrity the data is of no use.

2.2) Availability:

For any information system to serve its purpose, the information must be available when it is needed. Consider the case in which the data should have integrity and confidentiality. For achieving both these goals easily we can make those data off line. But then the data is not available for the user or it is not available.

III. HISTORY / HACKING TRENDS

In one early ethical hack, the United States Air Force conducted a "security evaluation" of the Multics operating systems for "potential use as a two-level (secret/top secret) system." With the growth of computer networking, and of the Internet in particular, computer and network vulnerability studies began to appear outside of the military establishment. Most notable of these was the work by Farmer and Venema, which was originally posted to Usenet in December of 1993.



(Source: The Cert® Guide to System and Network Security Practices)

Figure 1: Hacking Trends

International Journal of Ingenious Research, Invention and Development
ISSN (Online): 2583 648X

Volume 1 | Issue 2 | February 2023
Scientific Journal Impact Factor (SJIF 2023) = 3.647
DOI: 10.5281/zenodo.7821165

IV. CONCLUSION

One of the main aims of the seminar is to make others understand that there are so many tools through which a hacker can get in to a system. There are many reasons for everybody should understand about this basic. Let us check its various needs from various perspectives.

- **Student**
  A student should understand that no software is made with zero vulnerabilities. So, while they are studying, they should study the various possibilities and should study how to prevent that because they are the professionals of tomorrow.
- **Professionals**
  Professionals should understand that business is directly related to security. So, they should make new software with vulnerabilities as less as possible. If they are not aware of these then they will not be cautious enough in security matters.
- **Users**
  The software is meant for the use of its users. Even if the software menders make the software with high security options without the help of users it can never be successful. It's like a highly secured building with all doors open carelessly by the insiders. So, users must also be aware of such possibilities of hacking so that they could be more cautious in their activities. In the preceding sections we saw the methodology ofhacking, why should we aware of hacking and some tools which a hacker may use. Now we can see what can we do against hacking or to protect ourselves from hacking.

REFERENCES

[1] http://netsecurity.about.com
[2] http://researchweb.watson.ibm.com
[3] http://www.eccouncil.org
[4] http://www.ethicalhacker.net
[5] http://www.infosecinstitute.com
[6] http://searchsecurity.techtarget.com
[7] http://www.blackhat.com
[8] http://www.astalavista.com
[9] http://www.cert.org
[10] http://www.neohapsis.com
[11] http://packetstormsecurity.org
[12] http://www.securityfocus.com
[13] http://www.securitydocs.com
[14] http://www.foundstone.com