HACKING- A CHALLENGE TO INFORMATION SECURITY

Akanksha Bansal Chopra*

Abstract –

Information or data security is of high concern for almost all organizations. Hacking though can be dealt with use of firewalls, better and much improved ways of detecting intrusions through advanced software, but some non-technical issues may also lead to hacking, if are ignored. This paper attempts to discuss these non-technical issues, if are taken care off, may reduce the risk of hacking. Also the fundamentals of hacking are discussed.

A survey was conducted with 50 people. Questions regarding hacking were asked and responses were collected. The survey aims to study about the awareness of hacking among people with different age groups. Majority of targeted audience are IT professionals. The survey further aims to study different sources through which intrusion (hacking) is taking place in present scenario.

***Key word**: Hacking*

* Department of Computer Science, Shyama Prasad Mukherji College (Delhi University), Punjabi Bagh, New Delhi, India

1. Introduction

With the wider use, computer security has become an important issue for the organizations and government. These organizations are using Internet in their wide variety of applications such as electronic commerce, marketing and database access. But at the same time, data and network security is a serious issue that has to be talked about. The information such as credit card numbers ,telephone numbers, home addresses, bank account numbers etc. that are available on network may easily be hacked by unsocial elements. This is because of the increasing popularity and use of computers, access to them was limited to authorized or concerned personnel. But when some users were refused to access the computer, they would take it personally, and would challenge the access controls. They would steal passwords and other information by intruding into the system so as to take control of the entire system. They would do such things just to satisfy their ego of not been given the control to access the system, or just for fun, or for money[1].

Primarily, these computer intrusions were benign but now they have become a serious issue of security. Occasionally the less capable, or less cautious, intruders would unintentionally bring down a system by damaging its files. The system administrator would then have to resume and make repairs to the system. On the other hand, when these intruders were denied access, they would purposefully take destructive actions to harm the organization[1].

To start with hacking, initially organizations decided that the best way to recognize any intrusion into their network or system is to have their own trained professionals who would attempt to break into their systems and would identify, if there are any intrusion threats. These professionals, termed as “Red teams” or “ethical hackers”, follow same steps and tools as that of malicious hackers, but the difference is of there intensions. Ethical hackers have clear intensions to break computer security to save the organization from intrusion attacks. They never reveal the facts and information about the organization. But at any moment of time, if there intensions get sidetracked; they would be the one who would harm the most[1].

To prevent the information from being hacked, organizations recruit not only Red Teams but also use expensive hardware and software. Hacking could easily be avoided or could at least be reduced, if some precautions are taken such as not permitting any unknown or unauthorized person to access information. While using Internet, care shall be taken not to reveal personal information even if person on the other side is known to you.

2. Fundamental Principles of Hacking

A hacker is a person who enjoys learning the details of computer systems and enhances his capabilities. He is a computer enthusiast and extremely proficient in programming languages, computer systems and networks. Popularly, hackers are referred to someone who penetrates into computer network security systems. Ethical hackers, must be completely trustworthy. While testing security at client site they may discover almost all the data and that should remain a secret. If this information is leaked, then it may result in malicious hacking leading to organizations’ high financial loss. It is required that strong measures should be taken to ensure that the

information or data gathered during testing by the ethical hacker should not be leaked. This may be done, for example, by limited access labs with physical security protection, multiple secure internet and isolated networks for testing. The basic or fundamental principles – Accessibility, Confidentiality, Authenticity and Reliability, if are well understood and considered seriously by the organization, could reduce the risk to theft of their data and hacking. The fundamentals may be discussed as under:

Accessibility means that the information (or data) of the organization (or personal) is available. The accessible data should be secure and shall only be accessible by a valid user. The data, if accessed by any kind of outsider (semi outsider or total outsider), may lead to stealing of data followed by hacking. [1]A total outsider has very limited knowledge about the target systems. A well-defended system should not allow this kind of intruder to do anything. A semi-outsider has limited access to one or more of the organization's computers or networks. A valid user has valid access to at least some of the organization's computers and networks.

Confidentiality means that a secret data or information shall only be used, copied or accessed by a valid and authorized person. If the confidential data has been leaked to any outsider or unauthorized person then it is considered as a breach in confidentiality. This leads to intrusion into the system that is having confidential data and is followed by hacking. For example, permitting someone to look and giving access of your computer system may result in the theft of your confidential, private and secret data. If your laptop has physically being stolen, which again contains secret information say, financial information of your company, could result in a breach of confidentiality as the information may be with malicious hacker who may use this for his malicious purposes. Confidentiality is thus necessary for maintaining the privacy and secrecy of data to reduce malicious hacking.

Authenticity means that the data or information should only be revealed and disclosed to a valid user who has been authorised to control or access the data. The information if does not follow authenticity rule then the information would encounter a threat from a hacker, ultimately leading to a hacking, which may cause severe damage in the social reputation and financial growth of the company.

Reliability means that the data should not be changed, modified, updated, created or deleted without authorization. Only a valid and authorized user shall be given rights to make changes in the information. The information shall neither be shared on organizations' network without the permission of an authorized person dealing with it. A breach in reliability may result in intrusion of an outsider resulting in hacking.

3. Survey Interpretations

Keeping in mind the above fundamental principles of hacking a survey was conducted with 50 people regarding hacking. Data of only 32 found to be significant. A questionnaire containing 9 questions was given to them and the responses were noted and analyzed. In questionnaire, every question asked, was expected with a response only from the given options. The questionnaire has been included as an Annexure 1. The summary and purpose of th questionnaire is as follows:

Table 1: Summary of Questionnaire

S.No	Question	Purpose of Question
1.	User's Name	Parameter of Analysis
2.	Sex	Parameter of Analysis
3.	Age Group	Parameter of Analysis
4.	User's field of work	Parameter of Analysis
5.	User's place of birth	Parameter of Analysis
6.	Does user gets to know When someone other peeps In his system?	To obtain user's awareness about hacking
7.	User's interest in others' System	To obtain user's interest in hacking
8.	Method/source used for System	To study and rank different sources of hacking
9.	Person's who could be a threat to hacking	To study and rank different people, who may act as hacker

Below figure 1.1, shows the response sheet created after the compilation of the responses, given as answers by the people questioned.

S.No	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
1	Rupali	1	3	4	Satara	2	3	2,5	1,2,3,4
2	Naresh	2	6	5	HP	1	1	4	3
3	X	2	4	3	Delhi	3	3	0	1,3
4	Vaibhav	2	4	5	Delhi	5	2	6	1
5	Divya	1	4	2	Delhi	2	3	6	3
6	Archika	1	3	5	UP	2	3	5	1
7	Rakesh	2	3	2	HP	3	3	1,5	1
8	Pooja	1	4	3	Maharashtra	2	1	1	1
9	Y	2	3	3	UK	2	1	6,3	1,2,4
10	Suhas	2	3	2	Delhi	2	1	3,6	1,2,3,4
11	Pawandeep	2	3	3	Delhi	4	1	6	3
12	Megha	1	3	2	Delhi	2	1	2,3	4
13	Gaurav	2	4	5	Delhi	2	3	2,3,5,6	1,2,4
14	Prerna	1	3	5	UP	2	2	4,6	3
15	Piyush	2	3	3	Rajasthan	2	1	2	1
16	Manish	2	3	3	Delhi	2	3	3,5	3,4
17	Pawan	2	3	3	UP	2	3	0	0
18	Akanksha	1	3	2	Delhi	1	1	6,5	1
19	Mustafa	1	3	3	AP	4	3	0	1,2,3
20	Deepak	2	3	3	Delhi	2	3	5	1
21	Akhil	2	3	3	Delhi	4	3	3	1
22	Parul	1	4	5	UP	4	3	6,3,5	4
23	Rajesh	2	4	5	Bihar	2	2	2,3	1
24	Mukesh	2	3	3	HP	2	1	3	1,4
25	Unnat	1	3	5	Delhi	2	1	6	4
26	Surbhi	1	4	5	Delhi	3	1	6	1,2
27	Hemant	2	3	3	delhi	2	3	5	4
28	Tarun	2	3	2	Delhi	2	3	5	1
29	Aparna	1	3	2	Delhi	5	1	6	4
30	Nimish	1	3	5	Delhi	2	1	2	3
31	amanpreet	1	3	1	Delhi	4	3	5,6	1,3
32	Neelanshul	1	3	5	Delhi	4	3	5,6	1

Figure 1.1 Response sheet for Questionnaire

On the basis of the above response sheet, the frequencies are calculated against responses. Corressponding, frequency tables and charts have been created, as discussed below.

Table below, shows the frequency of responses, given against question numbers 6 and 7.

Table 1.1 Frequency table for question no. 6 and 7

	Very Rare	Rare	Never	Frequent	Very Frequent
Q6	2	19	3	6	2
Q7	13	3	16	0	0

Corresponding graph has been prepared and shown as figure 1.2(see online version for colors).

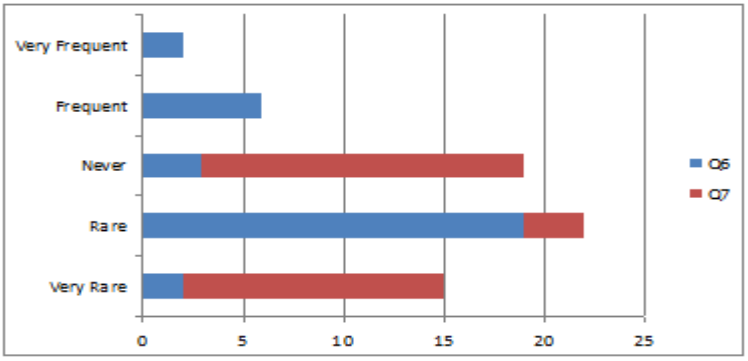


Figure 1.2 Frequency graph based on responses of questions 6 and 7

Table below, shows the frequency of responses, collected against question number 8. The options – Dial-up network, LAN, Physical entry, Social engineering, Directly through Laptop, Through Interrnet, have been considered as a variable X. Frequencies of each option has been noted as value for variable Y.

Table 1.2 Frequency table for question no. 8

X(options)	Y(frequency)
Dial-up network	2
LAN	6
Physical Entry	9
Social Engg.	2
Directly through Laptop	12
Through Internet	14
Total	45

Corresponding graph has been prepared and shown as figure 1.3.

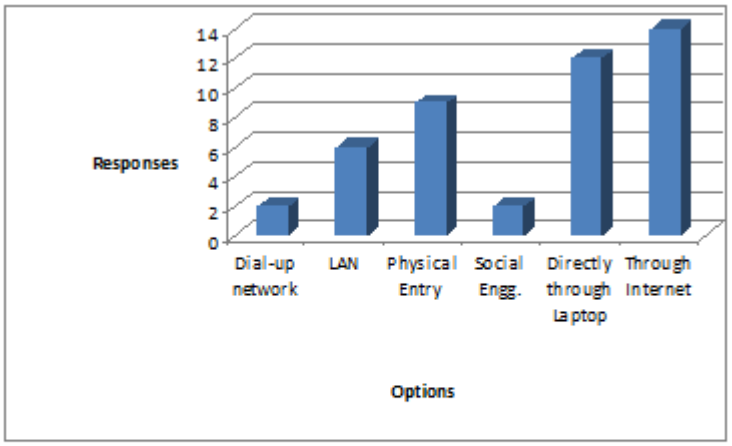


Figure 1.3 Frequency graph based on the responses of question 9

Table below, shows the frequency of responses, collected against question number 9. The options – An employee from same organization, an employee of other organization, person who often visits your organization and any other unknown person, are taken as variable X. Frequencies of each option are noted as value for variable Y.

Table 1.3 Frequency table for question no. 8

X(options)	Y(frequency)
An employee of your organization	20
An employee of other organization	6
A person often visiting your organization	11
Any other unknown person	11
Total	48

Corresponding graph has been prepared and shown as figure 1.4.

Figure 1.4 Frequency graph based on the basis of responses of question 10

4. Conclusion

The survey reveals that questions from 1 to 5 are only the parameters for analysis.

Question 6 and question 7 concludes that the young minds, i.e. age group between 20 years to 39 years are well aware about what is hacking. But the darker side is that instead of being aware about hacking they are neither alert nor serious for this severe aspect of computer world. This further concludes that they are neither prepared, if any attack is encountered.

Question 8, reveals and concludes that mostly, the source of hacking is Internet. In the present scenario, Internet has become a foremost and essential necessity but it should not be ignored that you are being watched for every single activity done by you on internet, by all kinds of hackers, i.e. total outsider, semi outsider and a valid user. This would result in intrusion into your system

and theft to data. Other sources of hacking are directly through users' laptop followed by physical entry of hacker to the users' place, through LAN, through Dial-up network and least with social engineering. Figure 1.5 shows ranking of sources, being used by hackers, in the scale of 1 to 6. Rank 1 is given the highest probability while rank 6 is given the least. This means that rank 1 specifies highest risk source of hacking while rank 6 specifies the lowest risk source of hacking.

RANK	SOURCE
1	Through Internet
2	Directly through Laptop
3	Physical entry to users' place
4	Through LAN
5	Dial-up Network
6	Social Engineering

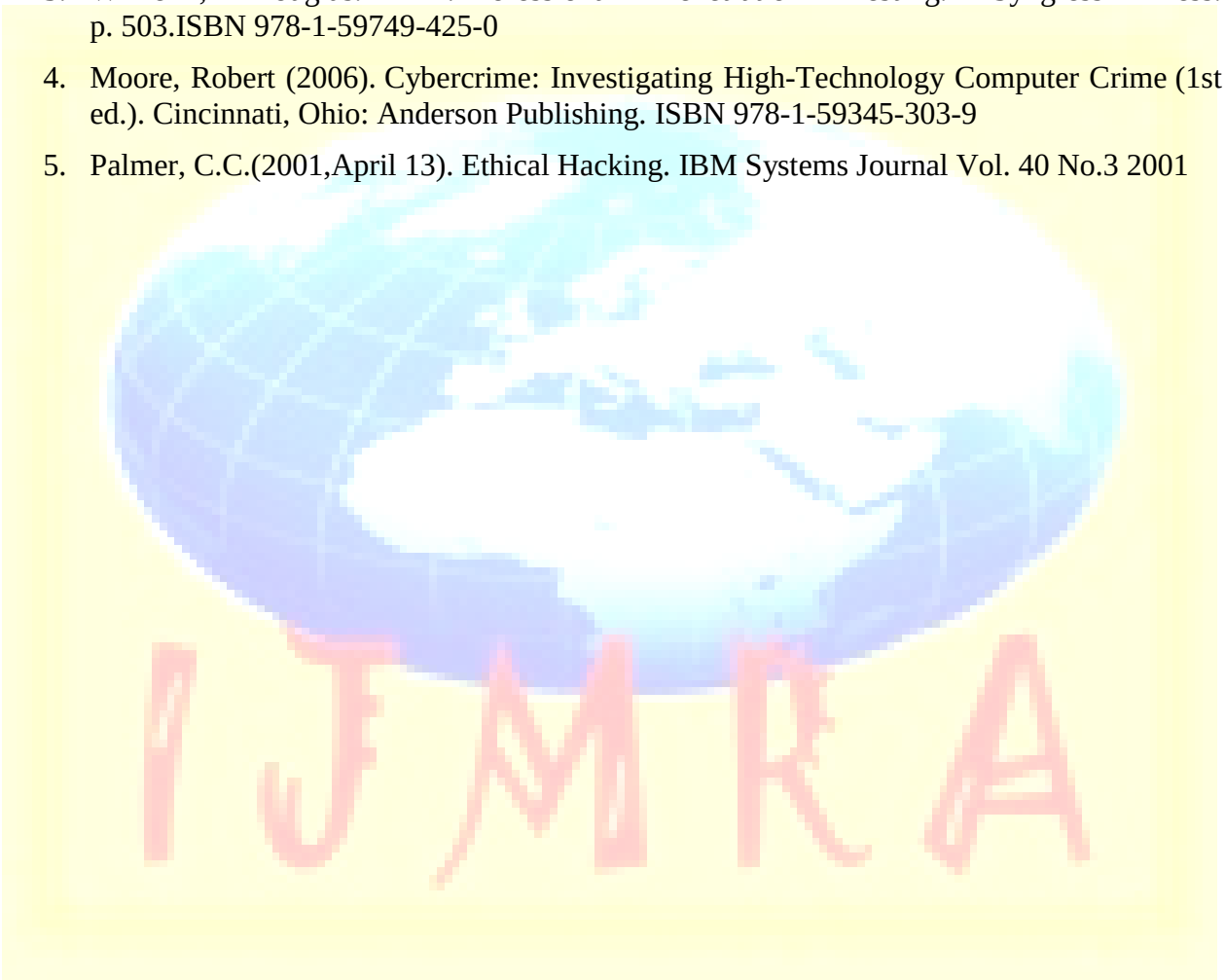
Figure 1.5 Hacking methods being used are ranked through 1 - 6

Question 9, studied for the person who can be of greater threat and responsible for intrusion into the system. The survey revealed that the person from the same organization is of great and much threat to the company for hacking. This is so because he will have most of the access to most of the data, which may create curiosity for him to intrude into the data. Moreover he will have the access rights of a valid user for the company's data so chances of being suspected get least. Other people such as any unknown person or any person who often visits your organization or any other organization employee are of less threat as compared to the one discussed above. These people will act as total outsider and thus do not have direct access rights to the data, leading to less interest and curiosity for intruding into the organization's data.

The survey and fundamental principles of hacking also concludes that in addition to technical protection such as protection through hardware or software programs against hacking, the risk to intrusion can be reduced and may be stopped at initial stages only, if above discussed issues are taken seriously and well treated.

References

1. Bansal, Akanksha, Arora, Monika. Ethical Hacking and Social Security. Radix International Journal of Research in Social Science Vol. 1, Issue 11, (November 2012), ISSN 2250 – 3994.
2. Arora Monika, Kanjilal Uma, Varshney Dinesh, An intelligent information retrieval: a social network analysis,Int. J. Web Based Communities, Vol. 8, No. 2, 2012.
3. Wilhelm, Douglas. "2". Professional Penetration Testing. Syngress Press. p. 503.ISBN 978-1-59749-425-0
4. Moore, Robert (2006). Cybercrime: Investigating High-Technology Computer Crime (1st ed.). Cincinnati, Ohio: Anderson Publishing. ISBN 978-1-59345-303-9
5. Palmer, C.C.(2001,April 13). Ethical Hacking. IBM Systems Journal Vol. 40 No.3 2001



Annexure 1

Questionnaire given to 50 people in the survey

1. What is your first name?

2. What is your gender?
1 female
2 male

3. Which category below includes your age?
1 17 or younger
2 18-20
3 21-29
4 30-39
5 40-49
6 50-59

4. What is your field of work?
1 Networking
2 databases
3 Development
4 Testing
5 others

5. What is your place of birth?

6. Do you get to know when someone other peeps in your work/system?
1 Very Rare
2 Rare
3 Never
4 Frequent
5 Very Frequent

7. Do you take interest in others' work/system without their permission/knowledge?
1 Very Rare
2 Rare
3 Never
4 Frequent
5 Very Frequent

8. Which method was used if your system was peeped in by someone else?
1 Dial-up network
2 LAN
3 Physical Entry to his place
4 Social Engg
5 Directly through Laptop
6 Through Internet

9. From below mentioned people, what do you think who can be a threat to your systems' information?
1 An employee of your organization
2 An employee of some other organization
3 A person who often visits your company for any reason
4 Any other unknown person