Journal of Science and Technology
ISSN: 2456-5660, Volume 6, Issue 6 (NOV-DEC 2021)
www.jst.org.in DOI: https://doi.org/10.46243/jst.2021.v6.i6.pp10-18

Fresh Perspective on Advancement in Methods of Hacking

Bansal S.K.[1]
[1](Department of Forensic Science, Chandigarh university, Mohali, Punjab, 140413, India)
Corresponding Author: bansalsid20@gmail.com

To Cite this Article
Bansal S.K., "Fresh Perspective on Advancement in Methods of Hacking", Journal of Science and Technology, Vol.6, Issue 6, NOV-DEC 2021, pp.:10-18.

Article Info
Received: 18-11-2021 Revised: 24-11-2021 Accepted: 01-12-2021 Published: 07-12-2021

Abstract: *Today, we are involve too much in technology, everything is available online. As, the dependency has increase, the number of users has also increase .people are using the internet for both constructive as well as destructive purpose. Some individual are using the networking system or internet either to violates or breech someone's privacy or to steal their personal sensible information. The main motive of this paper is to let people know about cyber and crimes related to it , hacking , hackers - their types, sections related to it and lastly the fresh perspective on advancement in methods of hacking .In this paper , some information regarding triangulation and onion shielding (the onion router or the onion theory) method are also explained. Various techniques of attacking or hacking like web jacking, e- mail bombing , trojan attack , DOS attack , DDOS attack , internet time theft , data diddling are also mentioned to enhance the knowledge. The methodology of this paper is based on review literature and further some fresh perspective and observations are added to it.*

Key Word*: Hacker , Hacking ,Web Jacking , E- Mail Bombing , Trojan Attack , DOS Attack , DDOS Attack , Internet Time Theft , Data Diddling , Triangulation and Onion Shielding Method.*

I. Introduction

CYBER CRIME ,Can considered as an. act in which the perpetrator usually uses the computer network and technology to either commit some offence against a person or a network

CYBER CRIMINAL, They are generally called as hackers, they via use of their device, often attack either a company or an individual or an organizational network for the purpose of benefit or defaming them by taking an access into their personal data or information.

HACKERS, A hacker is someone who knows various loop holes of a network or a software and methods of hacking. he uses his knowledge for breaching the protection of a device or a network and exploiting the information for various purposes.

Table no 1: Types of Hacking

ETHICAL HACKING	UNETHICAL HACKING
• Ethical hacking can be termed as , a legitimate task through which one can enter into the security of various systems or networks by which one can identify various loop holes that can be dangerous to the system or network. Usually the government agencies or the companies implies this type of hacking ,in which cyber security engineers are allowed to bypass the system security in order to ensure safety. This type of hacking is usually planned and is given authority by the law and is legal in nature unlike malicious hacking. • It is legitimate process.	Unethical means which is against the ethics of an individual, so in terms of hacking it can be defined as the hacking in which one uses his knowledge not for the constructive work but for destroying or exploiting the systems defence in order to get their own profit or defaming someone or gather the personal data or information. • • It is illegitimate process. • Use for destructive purpose. • It is used to gain the profit.

• Use for constructive purpose. • It is use to check the defence mechanism.	

Methods of Hacking:

This prospective comparative study was carried out on patients of Department of general Medicine at Dr. Ram Manohar Lohia Combined Hospital, Vibhuti Khand, Gomti Nagar, Lucknow, Uttar Pradesh from November 2014 to November 2015. A total 300 adult subjects (both male and females) of aged ≥ 18, years were for in this study.(10)

- Advantages in terms of hacker
- Disadvantages in terms of victim

Web Jacking:

Web jacking is originated from a word "HI- JACKING", it can be considered as an act in which an illegitimate control over the networks, web page by using their domain name system which creates a url and hence this URL made a parallel website of same look and preferences to attack the victim ,it is somewhere similar to phishing attack.

It is a type of hacking in which the theft is done in such a manner that the person who is not authorized to have the internet usage which belongs to some other person is using the internet connection whereas the person who is eligible gets another USER ID and PASSWORD foranother internet network connection.In this , the person who is the victim do not know , he is using someone else's internet connection illegitimate.

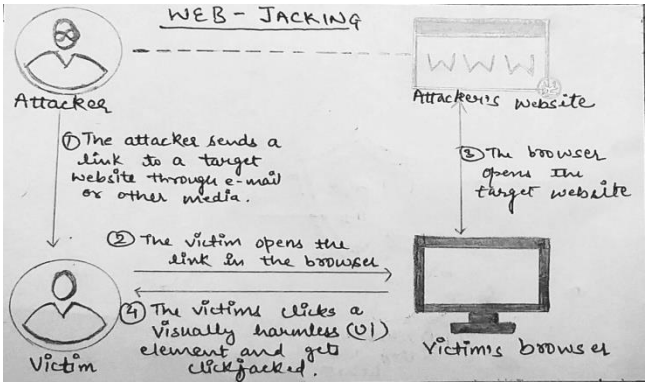

Figure no 1: Web Jacking

Advantages

- It is used to steal the sensitive data of the victim.
- Can make the illegitimate use of the steal data.
- Attacker can create a trap for the victim as in phishing does.
- By using this type of hacking, the hacker can do any illegitimate activity by using someone else internet connection so that later on while investigation this type of hacking can confuse the case , because it tampered the location and activity or performance of the actual perpetrator who is committing the crime.

Disadvantages

- Breech of personal information and other valuable documents .
- Can make manipulation in transaction Due to this type of hacking innocent might proven guilty
- Due to this hacking , a fraud case might get registered in the name of the victim who is been registered with the original internet connectivity .

II. Data Diddling

Data diddling can be referred to as diddling or illegitimately manipulating the data or information.

Prior to or while someone is entering into the system and further when the motive of the hacker is achieved then , this manipulated data can be bring back to its original form.

Or we can defined it as , when someone via means of virus or by manually alters or manipulate the program or the data and information and then can further bring it back to its original form.

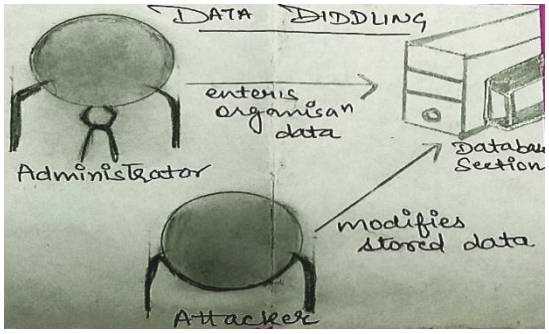

Figure no 2: Data Diddling

Advantages:

- This type of hacking can be used for the personal gain , so as the hacker can do the hacking to earn either fame or money or
- as well as this type of hacking can be used for the motive to made someone feel down or to target someone for the personal conflicts.

Disadvantages:

- In case of defamation , the identity of the victim might get defamed.
- Due to this type of hacking , false allegation can be made over the victim

III. DOS Attack

What happens in this type of hacking is that the cybercriminals will make the actual site not accessible for the genuine users.

A group of users start to make requests to the site from the same location to tie up that ultimately make the site non- responsive to the legal or actual users as they increase the traffic on that site or network.
These attacks are done to those sights that can be considered as the most visiting or high-profile sights.

DOS attack can be done through 2 ways-

- flooding services
- crashing services

there is one another kind of attack that is called as DDOS-Distributed Denial of Service attack in this type of attack the site is targeted by the users from multiple location and limiting it from being responsive to legitimate users.

Today technology can prevent the system or network from the DOS attack. But it is difficult to prevent from DDOS attack because it bears some unique characters

Advantages:

- Prevent the actual users from accessing the information present on actual site or network.
- Hackers are able to crash the site
- In case of DDOS attack it is difficult to identify the location from where attack is done, hence preventing the criminals from being caught.

Disadvantages:

- Loss of time and money for the person who is genuinely trying to access any network or site.
- Exploitation of vulnerabilities of a network or a system is done that will create problems for the actual users.

IV. Trojan Attack

It is a malicious code or we can say any software which will seem to the user as a legitimate but this software is able to take control completely over our system and after taking control it destroys our data.

At a particular instance the users will himself install this type of program in his device as it will seem to be a legitimate one to him. And after being install it will start to perform the action for which it was made. People might call trojan a virus but trojan has no such ability of replicating itself whereas a virus can replicate itself.
Some common types of trojan attack –

- RANSOMEWARE
- BACKDOOR
- MAILFINDER
- SPY
- EXPLOIT

Advantages:

- It can help a hacker in stealing the data and then asking money for that particular data.
- This type of hacking can be used for the personal gain, as the hacker will be successful in harming other

Disadvantages:

- The major disadvantage is loss of data.
- This might also cause loss of money to the victim.
- Privacy of the victim will be lost

V. Triangulation Method

With the advancement in technology , the method of hacking has also evolved Today, we have such a technology in which one person uses the GPS (GLOBAL POSITIONING SYSTEM) and VPN(VIRTUAL PRIVATE NETWORK) , to manipulate his/ her location , the person might be sitting in one location and in one just few seconds he might be in some other place or country as well , so due to this crucial advancement in technology , hackers are using this method to tamper their location , in order to protect themselves from being caught and also this method is proven successful for them too.

As, no current study can answer to this type of hacking that how to actually locate the real time location of the hacker , as there are lot of various other factors too , which are also playing role simultaneously .

Advantages:

- Due to the fluctuation in the location of the hacker , it is hard to locate the hacker t his real time loction and this being the greatest advantage

Disadvantages:

- The victim would not be able to get the justice because in this hacking, multiple location is been generated so it is harder to access the hacker and this can confuse the case.

VI. Onion Shielding Method

In this type of hacking method , the device protection is somewhere like cake, or smooth cream ,no both words are incorrect to define it , but it is just an imagination that looks like an onion ,a vegetable.

Like an onion which seems to be just a vegetable from its exterior , same is the case with the protective network that seems to be a normal protective measure from exterior .instead when we cut the onion into two halves , it shows the number of layers overlapping on each other ,and during this dicing of onion ,individuals tears roll down, thus the idea behind considering onion as imagination for protection system or network is similar to it , it's a protected by a layer on layer from inside.For the protection of our business or network , individual must use such a protective measure that will prevent your network by creating several.

Advantages:

- Because of multiple layer of protection, it is very difficult to locate the actual perpetrator .

Disadvantages:

- The victim would not be able to get the justice because in this hacking, multiple layers of protection is been generated so it is harder to access the hacker and this can confuse the case.

VII. Fresh Perspectives on the Advancement in Methods of Hacking

Before fresh perspective , I want to talk about the advancement in method of hacking , as the time evolving the technology and information is increasing day by day , thus this enhancing knowledge is used in both manner either for legitimate purpose or for illegitimate purpose.

The purpose of using this evolved information and technology is totally dependent upon the person or an individual that how and why and for what purpose he / she using this.

So, the motive or intension is one of the important factor that plays role ,or as we move towards hacking, it is already been defined that hacking in simple terms can be defined as the access to the computer system or devices or networks or website in order to either harm someone or save someone from fraud cases or from legal proceedings is known as hacking.

When this hacking is done to harm someone then this is known as unethical or illegitimate hacking or when this hacking is done for the purpose to serve someone justice or to save individual from fraud cases or legal proceeding in order to provide chain of custody or documentation in the court of law then this type of hacking is known as the ethical or legitimate hacking, these hackers serve their work in cyber security cell.

As with time , technology enhances with which the hackers are also coming up with new innovative hacking software , tools or devices in order to harm someone or to defame someone or to gain any personal profit or to gain money.

So to cope -up with these advancing problems or to stop the attack of hackers our government authorities like, cyber security hackers and also IIT software developer are working hard to prevent these attacks , they are developing the software ,which are going to work against these attacks.

There are numerous of hacking methods , from all of them here are 8 popular listed methods of hacking which are used by hackers generally , for hacking someone's accounts or network or database .

WEB JACKING	INTERNET TIME THEFT	DATA DIDDLING	TRIANGULATION METHOD
ONION SHIELDING	DOS ATTACK	TROJAN ATTACK	

In all these listed above hacking methods , the full-proof solution of some of the hacking methods have been developed and compiling with those ideas ,after making a deep research into software and languages, listed below are the methods to prevent the attack of these hacking .

- As we all know that each and every site has it's own IP address .thus , due to this IP address each web site has URL and also an DOMAIN NAME SERVICE/ SYSTEM.
- In this type of hacking , what hacker do in simple terms , lets consider an example of GOOGLE SITE, in this hacker will create an parallel web site which has similar looks as of the google site or google form , all functioning and everything will be same as of google but here by the use of Domain name service and create a fake URL , the hacker will hack the victims sensible information whenever the individual click on the fake URL of this parallel website , this fake URL is been transferred to the victm's device via e-mail , text messages , or on other social platforms or also by using pop – ups notifications .
- It is very easy to make the difference between the fake and original URL that is being generated by the websites , as of the basic indication to know whether the URL is fake or not is that , an original URL is never having any underscore (_) in it .
- Thus, the link or the URL having the underscore are not secure they are been considered as dangerous .
- Basically these links are made to steal or to breech someone's personal or valuable information or data in order to harm that person (as mentioned that motive of hacking is never be neglected) .
- Another way to differentiate between fake link and original link is that the original link is having the https;// (HYPER TEXT TRANSFER PROTOCOL) , when you double click on the link it will start surfing in your default browser , so at that time double click on link over the browser , if it shows the https then it is original otherwise that website is harmful to access.
- To prevent the device / system from the hacker and if your device or system or network or anything been hacked or you have feelings of this then you have numerous ways to get your privacy safe .
- One of the basic step that you can take is RESET YOUR DEVICE.
- Though , you can use any anti-virus in your system so as to prevent the system from any malicious attack .
- One of the paid and best anti-virus, during the research is BIT-DEFENDER, this anti-virus can do trouble shooting, and not only this anti-virus will detect the attack in the system but it also rectifies the issues it-self , it has the setting of both manually and automatically enabling.

- This anti-virus , can also finds any breeching of data and information and also the threats to the device or any spamming through e- mails can be detected and these attacks are been blocked by it .
- Have you ever seen , that on some of the websites it is been notified that YOUR CONNECTION IS SAFE !! , you know what is the reason of it ? , the reason of this pop- up is because of SSL – CERTIFICATE , which stands for SECURE SOCKET LAYER) .
- SSL CERTIFICATE , it's a program that provides encrypted cryptographic key to the server thus to secure it , one of the famous example of it is what's app , as it has the feature of end to end encryption , and also there are more sites and apps having this SSL certification.
- SYSTEM 32 – this is any device or system in – built feature for the storage , that is not known to everyone , it stores each and every bit of information that you have accessed in your personal computer , whenever you use it , so as whenever any attack is been identified , so as victim of the result of hacking of your system to protect the data or to ensure that your privacy would not steal , take the immediate action , by accessing this SYSTEM 32 , and remove and erase all the information .
- PROTON MAIL – this term is also not common for everyone as most of the users or victims do not know about this , but this proton mail is been used by hackers most of the time , in these type of mails , what all you can do is , you can create your e-mail which is end to end encrypted , in this proton mail , it will help you to generate a parallel mail with USERNAME and PASSWORD , so that by the use of this proton mail you can access any link or URL in case of fraudulent, where they will ask you to mention your e-mail or passwords.
- Due to the help of proton mail , the identity , personal information and other valuable and sensible information is kept safe , and thus it is really easy to create and access .
- Browsers like FIRE-FOX , have anti – phishing technology , due to which if you browse any fake or fraud website or link , it will automatically gets stop and thus won't open that link for you .
- There are numerous ways to access or hack someone's ID and PASSWORD on any social or online platform , some of the mentioned are – by phishing , by e- mail bombing or by carding method (ATM CADS – CREDIT AND DEBIT CARDS) ,, any hacker can access into your account by these methods and breech the identity .basically , when such type of hacking takes place this is termed as INTERNET TIME THEFT .
- In internet time theft , the hacker breech or harms the victims intellectual property , so as to prevent this attack you can change your password or can deactivate your account or by removing your personal information from that particular platform
- In case of ATM card hacking , you can lodge the FIR first , then move towards the blocking of the card , and use authentication factor so that only you can access to that particular account .
- Basically to prevent most of the types of hacking you can use end to end encryption , and also follows the same steps as mentioned above.
- TRIANGULATION and ONION SHIELDING METHOD ,are the methods that has been evolved in recent times and there is very less study for these methods.
- In earlier times, the hackers generally used to hack the system or network but as with the technology advancement they still used to hack the system but also they created several protection layers of firewalls , though due to which, it is near to impossible to access the exact location of the hacker.

VIII. Introduction to CIA Triad

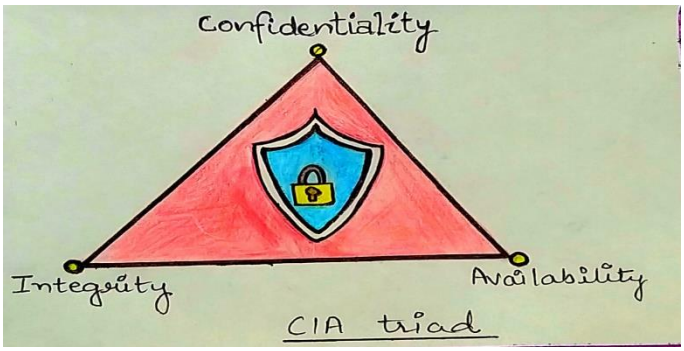

Figure no 3: CIA Triad

CIA TRIAD , this terms is stands for :-

- Confidentiality
- Integrity
- Availability,

This CIA triad model is made or proposed to check the guidelines which are related to cyber or digital networking security in an authority or in an organization.

Sometime this model is termed as AIC TRIAD model , because the term CIA is also stands for central intelligence agency .here also AIC means , availability , integrity , and confidentiality.

Though these elements of the triad are most common , important and functions demands of the digital protection and also for the updating of this CIA triad qualified professionals in the field of cyber security needs to effective and approachable and though knowledgeable.

Importance of CIA:

- As the each letter in the CIA triad , already indicating the basic and main functional principal of the cyber protection itself .
- In the informational protection , the most three important key aspects are confidentiality , integrity , availability .
- When all these three functional principal held together , they form a frame work and thus this is known as CIA TRIAD , and hence this triad combining together is used to keep the principles that are used for the guiding of the cyber protection .
- The value is been fallen into these three key elements , when the evaluation od demands and need are done and also here the study of cases is made so as to make an new outcome and technologies
- Thus this question is being asked by the CIA TRIAD that how the information is being classified .
- CIA TRIAD , it an interlinked triad , in this all three key elements are equally important and valuable for the organization
- None of one element can be use independently in the organization for keeping the sensible information .

Challenges Faced Bytriad of CIA:

Table no 2: Challenges Faced by Triad of CIA

When the size of data is very large it became very challenging for CIA triad to keep the track over it .
The size is date is very large because of the following reasons – Great amount of valuable information is required for the safety purposes of the authority . Multiplying the origination of the valuable information from where this sensible information is received. This sensible data exists in different – different formats .
ALREADY , existing huge prices is come in play when sets of information makes duplicate copies or due to the planning of recovery from any disaster .

All the interpretations from the sensible information is been made and collected with in the huge data , so that concerning with this large amount of data is important ,but due this amount and size of data the important and responsible information gets neglected .
INTERNET OF THINGS PRIVACY
INTERNET OF THINGS SECURITY

Forensic Significance:

- Digital , as a subject is very useful in forensics, it plays an important role in our judicial system .
- Day by day several internet frauds are incorporated in front of a cyber crime or forensic scientists.
- For this one must have a proper knowledge of the hacking technique as well as the hacking , so that one will be able to get the potential evidences of any crime.
- As forensic is based on proofs , so for getting the proofs in any cyber based crimes , a forensic expert must be aware of such tools and technologies that the perpetrator introduce to our system.
- Not only in unethical way , hacking also plays a major role in positive aspects that is ethical hacking where , the expert have to determine the various loop holes present in a system or device or when they have to trick a criminal at that point of time , hacking can also be used to manipulate the individual who is having a malicious motive.
- As we go further ,our society will completely be digitalized and thus , the digital crime is been increasing with days passing , each day an individual comes with either a new solution or new question to the expertise .
- The role of cyber forensics has increased to such an extent that it has become significant in our judicial system for criminals .
- Individual must involve these technologies as well as these disciplines of forensic in their knowledge so that they would be able to work efficiently and eminently .

IX. Case Study

Pune : Cosmo Bank Attack (2019)

- To target the users or to attack on the victim as with the technology advancement , the hackers or digital criminals have been using improvised tools and techniques.
- Various fields like business organizations , foundational authorities , and other sectors which are related to the digital technologies or who are using digital equipment to run their performance have been facing these cyber attacks.
- Similarly , in this case in 2019 , Cosmo bank in India has faced an malware digital attack.
- This attack took place on such large platform that it shocks the other banking authorities and companies related to it .
- In this attack , the cyber attackers or criminals or hackers drafts off rupees 94.42 crore
- This draft off of money is taken place in COSMO BANK CO. LD. In Pune in 2019 .
- Now the question raised that what did the hackers do ? who is the hacker ? how did he does this ? why did he done ?
- Hacker or the cyber criminal ,hi-jacks the server of the bank to hack the system to breech the personal data and sensible information, they also used to steal the information related to the visa card and the debit card holder's too .
- The money which is been draft off is of the people who are been situated in parts of other 28 countries .
- As soon as they got this information of this attack they withdraw the money , they have been deposited .
- Among the 28 countries , HONG KONG , INDIA , CANADA and other are also part of it .
- By using the compromising swift system an amount of 14 crore is been transferred to the Hong Kong bank
- Remain , amounting of 80 crore was been draft off by using the malware attack, as this virus is on gateway of visa and debit card .

- Previously , the Maharashtra governmental authorities and digital crime professionals have claimed that the reason behind this attack is a gang based on Lazarus from North Korea.
- Those who are been convicted are found to be money mules but the person who is having the hand and the master mind of this attack is not been caught yet .
- MALWARE ATTACK – this is a type of virus , which is been commonly used in digital crimes and by digital criminal for the context of breeching someone sensible data and information from the victim system.
- Some of the common examples are – SPYWARE , RANSOMEWARE
- Usually , hackers do this type of hacking to gain personal profit .
- CONCLUSION – hacking is not wrong process , until / unless your motive or intension is not .

X. Result and Discussion

Techniques like web jacking , internet time theft , data diddling , trojan attack , DOS AND DDOS Attack , e- mail bombing , their perspective are already been mentioned in many studies. A fresh perspective or new direction is given to these various methods of hacking, that will eventually helps in resolving more issues related to it.

The triangulation and onion shielding methods are the one which do not have too much to be studied , in this paper a fresh perspective has been given to them by the use of various software like (PTNG and triangulation monitoring or onion shield router) were used and also different languages like C++ , JAVA , PYTHON are used so that some sort of new software can be generated but no line of conclusion is made . On the basis of studies a perspective is drawn which says that the triangulation and onion shielding both methods can be used in combination as well , as both of these methods are been used for the tampering or hiding of the actual location of the hacker , due to continuous variations or changes made in the location by the use of VPN , it creates a shield of firewall , thus to get the access or to unhide the hacker's original location , experts need to break these shield but it is been seen that to break these shield of firewall is near to impossible .

XI. Conclusion

As the time evolving the technology is also upgrading with the increase in need of the technology, various risk factors are also increasing. This paper has very well explained about various security risks , that one might have digitally. A true explanation of the processing of different type of hacker is given in this paper along with the how various hackings are being done and what could be the advantages and disadvantages of them . today hacking is become common , the only difference between a good and bad hacking is of intent or motive of an individual . in the end this paper talks about the fresh perspective and various legal actions that are to be taken when someone violates or breeches the security aspects as mentioned in law .

References

[1]. Bansal, A., & Arora, M. (2012). Ethical Hacking and Social Security. Radix International Journal of Research in Social Science, 1(11), 1-16.
[2]. Hacking a paper by (Deepak Kumar, Ankit Agarwal, Abhishek Bhardwaj)http://www.ijcstjournal.org/volume-2/issue-6/IJCST-V2I6P2.pdf
[3]. Study of Ethical Hacking a paper by (Bhawana Sahare, Ankit Naik, Shashikala Khandey) http://www.ijecs.in/issue/v4-i4/68%20ijecs.pdf
[4]. "Hacking for Dummies" a book by Kevin Beaver, CISSP (Information Security Consultant).
[5]. H.M David, "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1, Feb 23, 2004.
[6]. Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala , "Ethical Hacking " , International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010
[7]. System Security and Ethical Hackingwww.ijreat.org/Papers%202013/Volume1/IJR EATV1I1018.pdf
[8]. Ethical Hacking Techniques with Penetration Testing www.ijcsit.com/docs/Volume%205/vol5issue03/ijcsit2 0140503161.pdf(by KB Chowdappa)
[9]. Hackers: Methods of Attack and Defense. Online. Discovery Communications.28Oct.2003 .