IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Role of Ethical Hackers in Digital Security Systems

Dr. Sonal Pathak[1], Mr.Vivek Malhotra[2], Mr. Gulshan[3], Mr. Asif Khan[4], Mr. Bhupesh Sharma[5]

[1]Associate Professor, Manav Rachna International Institute of Research & Studies, Faridabad

[2,3,4,5] Students, Manav Rachna International Institute of Research & Studies, Faridabad

Abstract

This paper explores the ethics which were immersed with a noble cause but lost the track of right direction and became the problem in the network security system. This subject has lots of controversies over the past few years. The question of true intention of an ethical hacker is still unsolved. Technology has developed the techniques but what about the true and loyal intention.

The study provides ethical evidence to the top management so that they can change policies and procedures to protect future generation. By studying all the aspects: 1) digital security measures 2) security software 3) the collective role of government, management, teaching staff 4) data models((i) Insider Attack Analysis, (ii) Blockage of backdoor leak by autonomic system) 5) Automatic tools, all have its own significance and its role in security system.

Collective measures in every field of digital/ cyber security are needed to form the policies and procedures. Digital and cyber awareness should reach to the weaker section of the society. Government's initiative can give revolutionary outlook to India. China's current attack on India has given us a reminder and need of digital and cyber security are the future fields where India has to pay more attention.

1.1 **Introduction**

Ethical hacking technology has become the need of computer industry. Each country has its very important and confidential data which has to be protected from unauthorized person. Different examples of such worries are before us as Islamic World has opened up websites which spreads wrong concepts and targets about their religion. Some of these websites establish cyber schools which teach hacking techniques. The problem of teaching students to hack is a serious issue. How can we judge the right intention of the user? Professionals and experts tried their efficiency to improve the operating system. They wanted to prepare the structure of skills which can perform multitask. Only acquiring knowledge in hacking in not enough and the trainers could not be blamed. Responsibility checks should be applied. For example, in loan system we see that bank does not take risk to pass a loan without guarantor. Here, other persons are involved for security purpose. If we apply such type of terms and conditions for eligibility of hacking course, the criminal data of hacker would automatically reduce.

Hackers in the form of cyber criminals reach into economic systems, our country's army/military system, use of weaponized information lies and propaganda to dangerously destabilize human groups are the serious issues which can ruin our economy and create challenge before our country.

DIGITAL SECURITY SYSTEM

Digital security refers to various methods which are used to protect your identity, assets and technology in the online and mobile world. Digital Security tools can be used to protect your identity including antivirus software, web services and secure personal devices. Smart card based token, sim card, e-passport digital security devices which comforts us in travel shop, work, and communication.

Digital security risks

1. Includes events causing loss or damage to hardware, software, data information and processing capability.
2. Computer crimes and internet based illegal acts.
3. Someone who access a computer in an unauthorized way risks from paid hackers to find vulnerabilities in systems and networks as part of cyber security consulting.
4. Corporate spies has advanced computer and networking skills which is unethically used to steal sensitive and confidential data and information.
5. Unethical employees who break into the company's network to access other computers on the network for financial gains.
6. Cyber terrorists use the internet to destroy.
   Cyberextortions

Security Systems

Physical security- servers are based in a secure data centre in Manchester. This is fully ISO 2 Toddle complaint and hardware is safely protected by several layers of security checks.

Virtual Security- Servers use firewalls to lockdown any vulnerable access points. This database use 128 bit encryption to your data safe. SSL(Security Socket Layer) certificates to further protect any privileged parts of an application.

Application design- Always use latest technology and follow the best practice so they can only be accessed from specific IP address or even provide an intranet based solution which is only available on a local network for the highest level of security.

Best Security software for windows 10,8,7:

1. AVG Ultimate
2. Norton Security Standard
3. Kaspersky Total Security
4. Bitdefender Internet Security
5. ESET Smart Security Premium
6. Avast Pro Antivirus
7. Trend Micro Antivirus Plus
8. Avira Antivirus

Ways to protect digital ecosystem

Choose a decent CMS platform- Most businesses built their digital ecosystem on CMS platform be sure to understand the available security feature and backend cybersecurity support for CMS platform and digital support team. Clients upload sensitive financial and personal data that can be misused by criminals if your CMS systems have poor quality security. Most important is to work with a team who understand digital security and how to configure a web server and CMS for best security practical.

Implement safe connection and channels, protocols like SSL and TLS provide security to computer networks connections and channel businesses use for operation. E-wallet implementing SSL and TLS protocols provide additional security to the financial transactions on your website. It saves data from fraud and theft.

Apply strong authentication protocols- To help and protect the customers data you can send log in alerts and notifications. Using passkey and strong passwords in the backend is another way to ensure security of OS

Take assistance from specialised cybersecurity system.

This includes sniffing your online banking details, email credentials and more of your personal data.

1.2 Literature Review

It is a demand of time, technology and country to obtain skills in ethical hacking to improve the vulnerabilities of a computer operating system. By knowing its dark side, we cannot stop giving education on ethical hacking, but can advice the students not to accept the slavery of unethical hacking and to be loyal to their conscious, otherwise if students/hackers have not adopted patriotic, ethical outlook towards this sensitive course then the unethical approach will steal the moral values from our life and left us abundant with criminal tendency. Our owners have to think that we have become body of human with deficiency of humanity and moral values.

And this damaged, unconscious, unethical structure of human will leave only destruction in the world of technology.

1. Education and training

   When the students acquire new skills. Their use could be in the right direction or wrong direction. Is there any policy which can stop the students not to take wrong direction. A criminal background check, the requirement of some sort of professional certification and student's interviews are few measures which can check their intention. In training courses that are available in the world the tough part is to understand the reason behind their interest in the course.

2. Trust on fake factors

   Online sites, web applications, operating systems, cloud, mobile apps have 90% possibility of hacking and cracking of secret data for disastrous purpose. As these sites does not have safe and secure approval protocols. Terrorists/criminals/hackers enter through these sites and applications and trap innocent students/public. Such sites, apps should be added some governments/strategies so that harmful contents and factors could be filtered easily.

3. Problem Inside or Outside: A suspension

   Major problem is to estimate and understand the insider attack. The reason for this attack may be financial gain, political causes, evil eye of enemy countries territories. Many companies deal with disgruntled websites companies/ persons to destroy the company or to make attempt to damage Indian economy. China's current attack on Indian Army tells us that Defence Ministry's confidential data has been hacked and why contracts between the countries have not made to combat secure technology on its priority and what the vulnerabilities that have dared the enemy countries to hack Defence Ministry, Railways, Ministry of Foreign Affairs, Ministry of Information and Broadcasting, Jio, Airtel, Cipla Companies. 40,000 Cyber attacks by Chinese hackers on IT Sector and Banking sector in 5 days(20 June to 24 June, 2020). If our plans and secure policies are hacked by enemy countries in the future they can easily occupy the Indian territories.

4. Managing Risk Factor

   We all know that ethical hackers are highly qualified. They get heavy amount for their services.

   They have potentials to remove the factors, causes and consequences of risk by exploring vulnerabilities. They can capture and identify benefits which they can share with directors of the managements of the company. With their contribution and cooperation to the security system, the companies conduct penetration tests which include sample cyber attacks on their own systems to make better security

enhancements patches. If these security issues are ignored and there is incomplete submission of security guarantee by the hacker by his mistake. This may lead to a state of less reliability on client side database security. If possible to rectify and improve these mistakes several guidelines are being recommended to the clients by the organization to safeguard their database. These may include to avoid accessing a website without secure http(like for example in case there is http instead of https).These may also include not to save password on the website. Data entry should be made only with user's authentication and authorisation. For example, for verification, generation of OTP(One-Time Password) is required

1.3 Role of an Ethical Hackers

1. To determine security measures for organization's information security system. Ethical hacking give direction to the companies whose measures are ineffective, outdated and which contain weak points that can be exploited.
2. To provide awareness about cyber criminals. By showing the hacker's techniques that can attack their system and could be dangerous for their business and methods to prevent the hackers.
3. Another objective of Ethical hacking is to prepare the firms to handle the cyber attacks. Security experts are better able to prepare for future attacks. Cyber attack techniques always change its format.
4. To secure banking through Ethical hacking.

   It identifies security vulnerabilities on banking systems from the loss of client's computer system and company's confidential data.

1.4 Types of Hackers

1. White Hat Hacker: The ethical hackers who hack computers of corporate companies to check for any loop holes in their security system. Their job is known as Penetrating Testing.
2. Black Hat Hacker: Hackers who do not take hacking job from companies but their target is to cause harm to them. To achieve their target they sabotage the systems so as to obtain information which includes bank information, personal details, phone numbers, etc.
3. Grey Hat Hackers: They are combination/hybrid of white hat hackers and black hat hackers.
4. Crackers: These could be college students who hack systems for personal use.

1.5 Operating Systems and tools used in Hacking

2. Backtrack Linux: First OS used for hacking. It is designed for hack by Offensive Security Organization of Israel Hackers.
3. Kali Linux: Widely used OS across the world for hacking the system. It contains much more advanced tools than Backtrack Linux.
4. Bugtraq: Bugtraq aimed at digital forensics, penetration testing, Malware Laboratories and is used by attackers. It offers tools like forensic tools,malware testing tools,IT tools,network tools etc.
5. Aircrack-ng: It can crack passwords of Wi-Fi networks which are WEP and Wpa/Wpa2 encrypted by brute forcing.
6. Sqlmap- sqlmap is available for linux , windows and mac. At present, it can hack MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, HSQLDB and Informix databases.

7. Parrot Security OS- It is suitable for both 32bit (i386) and 64bit (amd64), with a special edition it works on old 32bit machines (486)

8. CAINE(Computer Aided Investigation Environment): It provides a complete forensic environment with a friendly graphical interface.

INDIAN GOVERNMENT'S BAN ON MAXIMUM CHINESE APPS

As India and China's peaceful defence and commercial contracts has been breached so Government of India has banned 59 Chinese apps for security purposes. Camscanner and other Chinese apps can target the privacy of business account and can beat technological trends.

1.6 COMPANIES OUTLOOK ON AUTOMATIC HACKING TOOLS

Companies are talking about using automatic hacking tools instead of ethical hackers to find penetrability in their networks and software. They can execute an automated tool to find vulnerabilities with investment of less amount. Here are some other companies which cannot digest the long reports produced by automatic hacking tools. They make effort to decipher the data and what to do with the information.

These tools could be used to help, support a business's cyber security efforts. But these tools could not take place of the sophisticated and complex activities of a dedicated hacking teams. Hackers spend more time to bypass and penetrate system so that they can learn every bit and byte. Through this procedure they become experts in the business system and gather information they can find and use everything they learn to form a complicated activities of a dedicated hacking team. A tool cannot discover a situation that it is not programmed to find unlike a human who can observe, learn, identify and adjust.

LOTTERY E-MAIL SCAMS

Some fake brand names are used to trap a customer by text, email, message that they have won 1 crore lottery. To claim their price they have to fill necessary details like bank account number, PAN number etc. For this purpose they use fake websites and apps. The form which is filled by the victim are confirmed by hacker. Hacker's main purpose is to win the faith of victim. They are also convinced by saying that the lottery price would be collected by the winner only.

If the lottery amount is from another country the victim is asked to pay courier fees, tax in advance. It is not easy to prove citizenship of another country, necessary documents formality. Here, the victim could be robbed in two ways:

1. If the victim visit without any security it becomes risky to visit that place to collect the winning amount. Hackers gang can rob everything from the claimer.

2. He could be asked to prepare fake documents for which he will pay other amount.

1.7 DIGITAL ETHICAL HACKING IN MARKETING

Yahoo, MSN, Google, Facebook, Cubic Adbrite involved in online marketing networks has made digital marketing easy. It is cheaper as compared to offline approach. Many mega stores are applying it. Many fraud practices have been found. The incidents like misuse of bank accounts, fake news etc. are major obstacles in the progress of digital marketing at its initial stage. Many marketers use unethical means and techniques to approach the consumers. Misuse of IP address and email ids are shaking the faith of Indian consumers. Although companies are trying to give their best performance by testing, tracking and analysis. Still Customer and industrial outlook shows there are many discrepancies found between marketers and customers. With the effective marketing strategy, certain educational/commercial marketing websites have made a move by making screenshot barrier and content copying restrictions features by applying additional security techniques/features set-up on their website. And thus marketers find difficulties to perform their task. Here, the consumer can save himself through awareness.

In digital marketing, we can use push and pull advertising strategies. Now, the digital marketing has its ethical issue that it can formulate the pull function out of push. The consumer could be bombared with the information which actually he has not demanded. But he might feel it is pulled by him. Advanced technologies can make it possible and might be bringing results to the marketers. It still leaves a question as to how far it is ethical.

Required steps to handle safe digital marketing

1. Consumer's permission to marketer and marketing. If consumer is not showing interest and company is still delivering messages. In such case marketing looses its effectiveness.
2. Government should be strict toward fake advertisements and websites with malware or computer viruses blocked or removed from the websites in order to reduce the possibility of hacking.
3. Governments ethical code of conduct should be applicable in digital marketing.
4. Common and easy marketing structure which should be approved at national level and easy to understand by a common man.
5. Marketing should be based on consumer's awareness phase. For example, Metro travelling.
6. Free analytics programs for public awareness(in digital marketing).

1.7 GOVERNMENT'S ROLE IN SETTING HIGH STANDARDS ON ETHICAL NORMS IN TECHNOLOGY

1. Honour and Recognition package for encouragement in the field of ethical norms in technology so that ethical aspect of technology should be encouraged as a skill.
2. Compulsory subject should be declared in our Education Policy.
3. Film and cultural shows should also focus on the ethical aspect of technology so that an innovative and responsible message could be given to our society.
4. Strict Amendments in the Constituition against frauds done by ethical hacker.
5. Certification of Ethical hackers should be ceased for whole life if technological ethics are breached.
6. Lifetime imprisonment, heavy security and mortgage rules for ethical hacker if something went wrong.
7. Citizenship should be cancelled for whole life.
8. If these strict and hard rules and regulations are applied by government, only the honest and trustworthy talent would come in this field.

1.8 Control Measures for Digital Hacking

The following model is an approach to monitor employees closely to reduce the risk of impact. It will also help in identifying implications early enough to reduce the impact of confrontation. This model could be used in workplace and also in the field of education. Another security solution could be to automate ethical hacking in allowing machines take over jobs of humans, the biggest problem that lies here is that machine are prone to making mistakes.

Figure for solutions

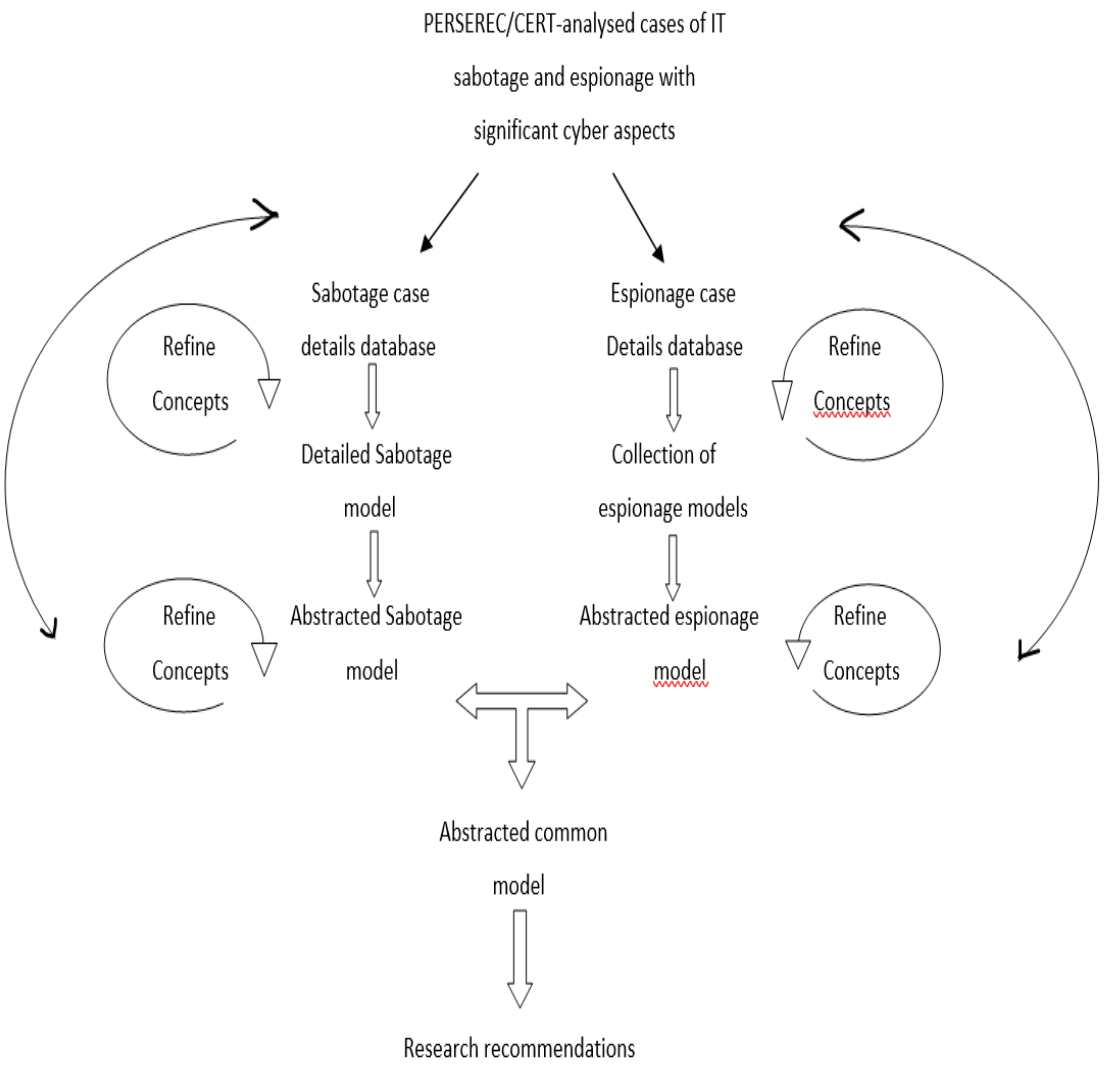

Figure 1: Insider attack analysis

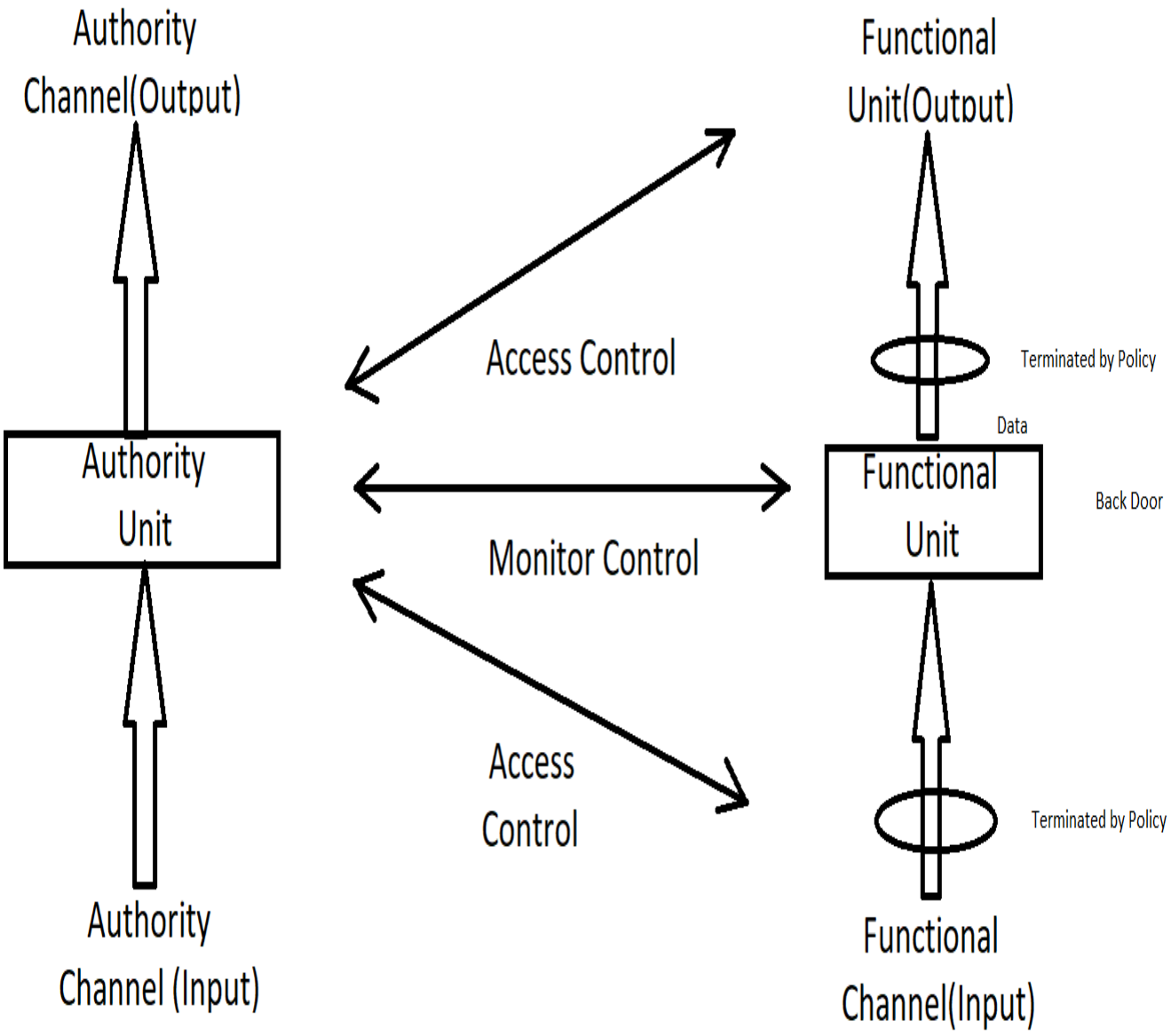

Figure 2: Blockage of backdoor leak by autonomic system

Explanation:

To make the operations trustable and strong, this feature(autonomic) follows best ways to control the working/functioning of each part/element/component, this standard has broad and self-controlled systems. To fulfil the safety need of the usage applications, this feature is also made.

Management Unit- Higher Authorities, CEOs, Managers, directors of the Company, Organization, Bank.

Functional Unit- Staff members, workers, clients in the office.

For example,

Input is given in the functional channel.

Cashier collects the cash, makes entry on the bank's software

If he seeks and tries to become clever by leaking the data to other enemy bank or organization for wrong/illegal purpose which may be financial or unethical. This is **Data Leakage through Backdoor**

He cannot do that because the higher authority or the manager has the access control over the sensitive data.

The control for using the organization's information is limited by the security experts of the organization by implementing the necessary policy.

While working, to fix the problem that the staff does not make cyber mistakes like by Facebook etc.

Control on them is managed and monitored regularly.

This policy control blocks the outgoing of sensitive data of the organization. And then, each staff member and the organization successfully achieves the output without any problem.

The Management Unit is itself a self-controllable element as it employs machines

Two issues

1. Higher management such as SEOs, CEOs are self-controllable with the use of ethical hacking by ethics of its policies in the organization. Ethics are implemented in the organization to make learn the employees, staff members, and the directories.
2. Higher Management is self-controllable without the help of ethical hacking.

Two processes/figures explanation

1. Database details of damage case(malfunctioning of computer through virus spread by attacker on the website or organization's server) are collected.
2. Based on the details of the sabotage(damage) cases which are collected and informed. Sabotage model is made/formed. These are re-refined, checked again and again, refreshed again and again.

Now, to judge the behaviour of the ethical hacker

There is a similar process in both the cases of damage and spying are judged and investigated.

In this process, first they are collected in a database. Then models suitable to their condition and nature are collected. Then, these models are abstracted after which researchers does research and deep study on it. Then by referring this research and deep study, they makes and prefers related recommendations to the IT Professionals who after verification forwards the same to the organizations to include in its policy for implementation.

//An abstract model in computer science is for greater importance on necessary details by removing unnecessary physical, spatial or temporal details or attributes are removed.

Process of reorganizing behaviour from non-abstract classes to abstract classes.//

Note: In every process, there are refining of concepts for clear and accurate data.

So, this was all about insider attack analysis.

As details of the attacker is not easy to find, several technologies like PERSEREC/CERT are used.

Example - of mirror from front-end and back-end.

Now, to improve security, some organizations wants to replace humans with machines as it is assumed that these machines give accurate results and builds firewalls more accurately than humans. The machines have one disadvantage that on damage they may not give accurate results as expected.

1.9 Conclusion

As India's ethics and morals have diverted the attention of other countries, it is hoped that revolution of ethical reforms in technology has started. Dignity of a country should be measured by technological progressive means or by ethical standards of technology.

If WHO have taken such hard and authentic restrictions on ethical aspect of technology. The world would not have to suffer from COVID-19 Epidemic because ethical norms of technology are breached and the world is suffering.

References:

1. Prof Suriya Begum*, Sujeeth Kumar, Ashhar," A COMPREHENSIVE STUDY ON ETHICAL HACKING", INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH, ISSN: 2277-9655
2. www.google.com
3. www.appinonline.com
4. Ethical Customer Relationships: A Comparative analysis of US and French Organisations using Permission-based Email Marketing". Journal of Database Marketing, 10(1),53-59.
   Is the Internet more effective than traditional media? Factors affecting the choice of media. Journal of Advertising Research,41(6),53-60
5. D. Farmer and W.Z. Venema, "Improving the Security of Your Site by Breaking into It," originally posted to Usenet (December 1993)
6. S. Band, D. Cappelli, L. Fischer, AP. Moore, RF. Trzeciak and E. Shaw, "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis", Carnegie Mellon University, 2006.
7. The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws- Book by Dafydd Stuttard and Marcus Pinto
8. Black Hat Python: Python Programming for Hackers and Pentesters- Book by Justin Seitz
9. Hacking Computers- Book by T. Norman
10. The Unofficial Guide to Ethical Hacking- Book by Ankit Fadia
11. https://www.tutorialspoint.com/ethical_hacking/index.htm