Mahatma Gandhi Mission's

College of Computer Science & IT, Nanded.

Department of Computer Science & Information Technology

2020-2021

Seminar Synopsis

Ethical Hacking

Submitted by

Zeba Khanum

Under the guidance of

Mr.Dahale S.V.

Ethical Hacking

What is hacking?

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system.

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

Ethical Hacking:

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, to minimize or eliminate any potential attacks.

In the ethical hacking we have to make sure about the security of the system as far as information technology is concerned. As the name says itself ethical hacking, it has two meanings or definitions one which is the hobby or profession of a particular person who is interested to make career in this field. Another one who is breaking one’s system for a purpose. Well the first definition has become older in today’s scenario whereas the second one has a meaning. The hacker culture began in the 1960s and 1970s as an intellectual movement: exploring the unknown, documenting the arcane, and doing what others cannot. It is actually a way to do the security assessment which can be checked from the technical point of view.

Types of Hacker:

1. White Hat Hackers
2. Black Hat Hackers
3. Gray Hat Hackers
4. Script Kiddies
5. Green Hat Hackers
6. Blue Hat Hackers
7. Red Hat Hackers
8. State/Nation Sponsored Hackers
9. Hacktivist
10. Malicious insider or Whistleblower

Goals of System Hacking:

1. Gaining Access
2. Escalating privileges
3. Executing applications
4. Hiding files
5. Clearing tracks

Advantages of Ethical Hacking :

Following are the advantages of Ethical Hacking as follows:

- This helps to fight against cyber terrorism and to fight against national security breaches.
- This helps to take preventive action against hackers.
- This helps to build a system that prevents any kinds of penetration by hackers.
- This offers security to banking and financial establishments.
- This helps to identify and close the open holes in a computer system or network.

Disadvantages of Ethical Hacking :

Following are the disadvantages of Ethical Hacking as follows:

- This may corrupt the files or data of an organization.
- They might use information gained for malicious use. Subsequently, trustful programmers are expected to have achievement in this framework.
- By hiring such professionals will increase costs to the company.
- This technique can harm someone’s privacy.
- This system is illegal.