SNS COLLEGE OF TECHNOLOGY

DEPARTMENT OF MCA

COMPUTING ETHICS – III SEMESTER

TWO MARKS QUESTIONS & ANSWERS

UNIT II: COMPUTER HACKING

1. Who are called Hackers?

- A person who enjoys learning the details of computer systems and how to stretch their capabilities, as opposed to most computer users who prefer to learn only the minimum amount necessary.
- Someone who programs enthusiastically, or who enjoys programming rather than just theorising about it.
- A person who is able to create programs quickly.
- An expert on a particular program, or one who frequently does work using it, or on it.

2. State the motives behind hacking.

Some of the motives behing hacking are

- Vandalism – Criminal behavior
- Public interest
- Reveal wrongdoing
- Financial gain
- As a protest
- The challenge (fun)

3. What is Virus?

A virus is a self-replicating piece of programming code inserted into other programs to cause some sort of unexpected, and usually undesirable event.

4. Give the names of some viruses.

- Trojan horses
- Worms
- Time or logic bombs
- Denial-of-service

5. What is Trojan horse?

A Trojan horse, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data and possible system harm.

6. What is computer worm?

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

7. What is logic bomb?

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

8. What is time bomb?

A time bomb refers to a computer program that has been written so that it will stop functioning after a predetermined date or time is reached.

9. What is meant by Denial-of-Service?

Denial-of-Service(DoS) is an attempt to make a machine or network resource unavailable to its intended users.

10. List down the five principal values of hacker ethic.

The hacker ethic was comprised of five principal values :

- Access to computers, and anything which might teach you something about the way the world works, should be unlimited and total. Always yield to the hands-on imperative.
- All information should be free.
- Promote Decentralization
- Hackers should be judged by their hacking, not bogus criteria such as academic excellence, age or position.
- Can create art and beauty on a computer.

11. Define 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 way past the 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, in an effort to minimize or eliminate, any potential attacks.

12. What constitutes ethical hacking?

In order for hacking to be deemed ethical, the hacker must obey the following rules:

- Expressed (often written) permission to probe the network and attempt to identify potential security risks.
- You respect the individual's or company's privacy.
- You close out your work, not leaving anything open for you or someone else to exploit at a later time.
- You let the software developer or hardware manufacturer know of any security vulnerabilities you locate in their software or hardware if not already known by the company.

13. What is meant by Cracker or Cracking?

According to Ralph D. Clifford, a cracker or cracking is to "gain unauthorized access to a computer in order to commit another crime such as destroying information contained in that system".

14. What is meant by Spyware?

Spyware is any software that secretly gathers user information through the user's internet connection without the person's knowledge, usually for advertising purposes.

15. What are the classifications of Hackers?

White hat

A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker

Black hat

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain"

Grey hat

A grey hat hacker is a combination of a black hat and a white hat hacker. A grey hat hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. They may then offer to correct the defect for a fee.

16. What are the various possible techniques of computer security attacks?

Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Firewalls defend computers from intruders by limiting access to ports and machines, but they can still be circumvented.)

Finding vulnerabilities

Hackers may also attempt to find vulnerabilities manually. A common approach is to search for possible vulnerabilities in the code of the computer system then test them, sometimes reverse engineering the software if the code is not provided.

Brute-force attack

Password guessing. This method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used, because of the time a brute-force search takes.

Password cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. Common approaches include repeatedly trying guesses for the password, trying the most common passwords by hand, and repeatedly trying passwords from a "dictionary", or a text file with many passwords.

Packet analyzer

A packet analyzer ("packet sniffer") is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack (phishing)

A spoofing attack involves one program, system or website that successfully masquerades as another by falsifying data and is thereby treated as a trusted system by a user or another program.