Assignment No: 1

Page No.
Date

Q1 What is ethical hacking & explain types of hacking?

-> - Ethical hacking is also known as White Hat Hacking or Penetration Testing.
- Ethical hacking involves an unauthorized attempt to gain unauthorized access to a computer system or data.
- Ethical hacking is used to improve the security of the systems and networks by fixing the vulnerabilities found while testing.
- Ethical hacker improve the security posture of an organization.
- Ethical hacker use the same tools, tricks, and techniques that malicious hackers used, but with the permission of the authorized person.
- The purpose of ethical hacking is to improve the security and to defend the systems from attacks by malicious users.

* Types of Hacking

- Network Hacking

Network Hacking means gathering information about a network with the intent to harm the network system and hamper its operations using the various tools like Telnet, NS lookup, Ping, Tracert etc.

2. Website hacking

W.H means taking unauthorized access over a web server, database, & make a change in the information.

Computer hacking

C.H means unauthorized access to the Computer & steal the informat^n from PC like computer ID & password by applying hacking methods.

Password hacking

P.H is the process of recovering secret passwords from data that has been already stored in the computer system.

- Email hacking

E.H means unauthorized access on Email account & using it without the owner's permissions.

Q.2] What is a purpose of Hacking? Write Advantages & Disadvantages?

→ Purpose of Ethical hacking

- The purpose of ethical hacking is to find and fix security weaknesses in computer systems, networks, & software before bad actors can exploit them.
- Ethical hackers use their skills to help organizations improve their cybersecurity defenses & protecting sensitive info^n from being stolen or compromised.

- It's like being a friendly digital detective, making sure everything is safe & secure in the digital world.

- Advantages
  - It is used to recover the lost of info", especially when you lost your password.
  - It is used to perform penetration testing to increase the security of the computer & network.
  - It is used to test how good security is on your network.
  - E.H helps identify & fix vulnerabilities, making system more secure against malicious attacks.

- Disadvantages
  - It can harm the privacy of someone
  - Hacking is illegal
  - Criminal can use hacking to their advantages.
  - Hampering system operations.

Q.3 Explain types of hackers & code of ethics?

->- Black Hat Hacker

- Black Hat Hacker are also known as an Unethical Hacker or a Security Cracker.
- These people hack the system illegally to steal money or achieve their own illegal goals.
- They find banks or other companies

with weak security & steal money or credit card information.
- They can also modify or destroy the data as well. Black Hat hacking is illegal.

White Hat Hacker

- W.H.H are also known as Ethical Hacker or a Penetration Tester.
- W.H.H are the good guys of the hacker world.
- These people use the same technique used by the black hat hackers.
- They also hack the system, but they can only hack the sys. that they have permiss^n to hack in order to test the security of the system.
- They focus on security & protecting IT sys. W.H.H is legal.

- Gray Hat Hacker
- Gray H.H are Hybrid bet^n B.H.H & W.H.H.
- They can hack any sys. even if they don't have permissi^n to test the security of the sys. but they will never steal money or damage the sys.
- In most cases, they tell the administrator of that sys.
- But they are also illegal as they test the security of the sys. that they don't have permission to test.
- G.H.H is sometiagmes acted legally & sometimes not.

Page No.
Date

* Code of ethics
- Now computer security training organizations have an ethical code of conduct that people must agree to abide by in order to be certified by them.
- The most popular hacker code of ethics on the Internet is the EC-Council Code of Ethics.
- It's a good code of ethics, but a bit too focused on penetration testing, and it's growing a bit long over time.

Q.4 Explain type of attacks & attack vectors types explain in detail?
-> Types of Attack- *Malware-
- A form of malicious SW that is intended to harm computers, networks & servers is known by the name Malware.
- Malware comes in many types, including Trojans, viruses, & worms, and all of them replicate & propagate through a device or network.

* Phishing
- A phishing attack convinces a victim to download malware or provide personal info" on spoofed websites.
- The attacker creates messages that look genuine & might appear to be form a trusted source, and then launches the cyberattack via email.

Page No.
Date

- DoS (Denial-of-Service)
= A denial-of-service (DoS) attack, also known as a brute-force attack, is used to prevent online service from fundioning properly.

- Man-in-the-Middle (MitM) Attack
In this scenario, an attacker intercept communication between two parties to eavesdrop or manipulate the data being transmitted.

- Cross-Site Scripting (XSS)
XSS attacks inject malicious scripts into web pages viewed by other users, compromising their browsing experience or stealing sensitive information.

- SQL Injection
This involves exploiting vulnerabilities in web applications to execute malicious SQL commands & gain unauthorized access to a database.

+ Types of attack vectors
- Compromised Credentials
- Usernames & passwords are still the most common type of access credential & continue to be exposed in data leaks, phishing scams & by malware.
- When lost, stolen or exposed, credential give attackers unfettered access.

- Weak Credentials
  - Weak passwords are reused passwords mean one data breach can result in many more.
  - Teach your organizations how to create a secure password, invest in password manager or a single sign-on-tool, and educate staff on their benefits.

- Malicious Insiders
  Disgruntled employees can expose private information or provide info^n about company specific vulnerabilities.

- Missing or Poor Encryption
  - Common encrypt^r method like SSL certificate & DNSSEC can prevent man-in-the-middle attacks & proted the confidentiality of data being transmitted.
  - Missing or P.E for data at rest can mean that sensitive data or exposure of credentials in the event of a data breach or data leak.

- Misconfiguration
  Misconfiguration of cloud service, like Google, Cloud Platform, Microsoft Azure, or AWS, or using default credentials can lead to data breaches & data leaks, check your S3 permissions or someone else will.

Page No.
Date

Q.5] Indian IT act 2000 & amendments Indian IT act 2008?

-> The IT act, 2000 (IT) is an Indian legislation enacted to provide legal recognition for transactions carried out electronically.
- It addresses various aspects of electronic commerce, digital signatures, cybercrime & data protection in India.
- Over the years, several amendments have been made to the IT Act to address emerging challenges in the digital realm.
- One significant amendent was made in 2008. Here's is an overview.

- Information Technology (Amendment) Act, 2008:
The IT (Amendment) Act, 2008 was passed by the Indian Parliament to update and strengthen the provisions of the IT Act 2000.

* Section & punishments under I.T. Act 2000 are as follows;

- Section 43
This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.

Page No.
Date

- Section 43A

This section of IT Act 2000 states that any corporates body dealing with sensitive info^n that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.

- Section 66

Hacking of a computer sys. with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs. 5,00,000 or both.

- Section 66 B, C, D

Fraud or dishonesty using or transmitting info^n or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.

- Section 66 E

Violation of privacy by transmitting image of private area is punishable with 3 years imprisonment or 2,00,000 fine or both.

- Section 66 F

Cyber Terrorism affecting unity, integrity, security, sovereignty of india through digital medium is liable for life imprisonment.