# INC - 402
# ASSIGNMENT

NAME: Parth Sarathi Yadav

BRANCH: CSE - AI

ROLL.NO: 2200521520035

—— x —— x —— x ——

(Ans1) An HTTP error 404 indicates that the server cannot find the requested resource. This could be due to various reasons such as the ~~*~~ resource being moved or deleted, or the URL being mistyped.

Error 404 Hacking Digital India Part Chase I!

→ Creating a trojan file such as android.apk file that will be distributed all over the internet and the person whoso ever download this file.

→ There are always bounded with other games.

→ we may never know that but that file may certain backdoo

⇒ once data is encrypted then it will ask for decryption passwords.

→ The key will be only when you pay a certain amount of money.

—— x —— x —— x ——

(Ans2) Control hijacking involves gaining unauthorized Control over a computer system or program. Buffer overflow, ~~attacks~~ format string and Integer overflow attacks are common methods used in Control hijacking. Buffer overflow exploits the vulnerability of a program by overflowing the buffer with more data than it can handle, leading to the execution of arbitrary code. Format string attacks exploit the use of improper format strings input in programming languages like C, potentially allowing an attacker to read or write arbitrary memory.

—— × —— × —— × ——

(Ans3) Computer security threats encompasses a wide range of malicious activities aimed at compromising the confidentiality, integrity or availablity of computer systems and data. These threats include malware, phishing, social engineering, insider threats etc. Attacks can be launched to steal sensitive information, disrupt operations, or gain unauthorized access.

—— × —— × —— × ——

(Ans4) SQL injection is a technique used to exploit vulnerabilities in web applications that interact with databases. Attackers inject malicious SQL code into input fields, allowing them to manipulate the database or execute arbitrary SQL commands.

Denial of Service (DOS) and distributed denial of service (DDOS) attacks aim to disrupt normal functioning of a computer network or service by overwhelming it with a flood of traffic. Preventive measures for such attacks include input validation parameterized queries, rate limiting and deploying firewalles or intrusion detecting systems.

---

(Ans 5) Security models provide frameworks for implementing Security policies and mechanisms to protect computes Systems and data. Different models include the Bell-La Padula model, Biba module, Clark wilson- model an Brewer Nash mode, and also known as the chinese wall model. Each model has its own set of rules and principles governing access control and information flow.

---

(Ans 6) The UNIX / LINUX security architecture involves various components and mechanisms to safeguard the operating system and its resources. This includes user authentication, file permissions, access control list (ACL s), security -enhanced Linux (SE Linux), mandatory access control (MAC), and auditing. Additionaly, unix/ Linux systems often employ firewalles, intrusion detections/ prevention systems, and regular software ~~std~~ updates to mitigate security risks.