Day 1

VAPT: Vulnerability Assessment and Penetration Testing

Cyber Security: practice of protecting systems, networks and programs from digital attacks which are usually aimed at accessing, changing or destroying sensitive info.

Types of Attacks

-> **Phishing** [practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card and login info.]	**-> Ransomware** [A type of malicious software which is designed to extort money by blocking access to files or the computer until the ransom is paid.]	**-> Malware** [A type of software designed to gain unauthorized access to or cause damage to a computer.]	**-> Social Engineering** [Manipulation technique that exploits human error to gain private information, access or valuables.]	**-> Man in the Middle** [The criminals interrupt the traffic between a two-party transaction. He can read all the data packets and can redirect all the traffic through his system.]	**-> Zero day** [A zero-day attack is a hack that uses a previously unknown software flaw before the vendor knows about it, allowing no time for a fix.]

USB Rubber Ducky: A social engineering device crafted in the shape of a pen drive; mainly used to gain access to the computer in which it is plugged in.

Cookie: A browser cookie, also known as an HTTP cookie, is a small text file sent from a website and stored in a user's web browser. It contains data to enhance user experience, provide personalized services, and remember user preferences. Importantly, cookies are not executable code and do not harm the user's device or compromise security.

Ethical Hacker: A professional having excellent knowledge and skills on identifying and exploiting vulnerabilities. He works with the permission of owners of the system and must comply with the rules of the target organization. Their aim is to assess the security posture of a target organization.

Types of Hackers

-> **White Hat** [An ethical computer security expert who uses their skills to identify and fix security vulnerabilities, rather than exploiting them. They follow a code of ethics and often work in roles such as penetration tester or cybersecurity consultant.]	**-> Black Hat** [A malicious computer user who exploits security vulnerabilities to gain unauthorized access to systems, with the intent to cause harm or steal sensitive information. They operate outside the law and ethical guidelines.]	**-> Grey Hat** [They often find vulnerabilities without malicious intent but may exploit them without permission. Their actions are not intended to cause harm, but they do not have explicit permission, which can put them at odds with the law.]	**->Hacktivist** [An individual who uses hacking techniques for political or social activism. They aim to draw attention to a cause, often by exposing information, disrupting services, or defacing websites. Hacktivism can be seen as a form of digital protest.]	**-> Script KIddie** [A "script kiddie" is a term often used in the hacking community to describe an inexperienced hacker who uses pre-written hacking tools without fully understanding how they work implying a lack of skill and knowledge.]

Types of Cyber Security Teams

RED	BLUE	PURPLE
• Offensive Security • Ethical Hacking • Exploiting Vulnerabilities • Penetration Tests • Black Box Testing • Social Engineering • Web App Scanning	• Defensive Security • Infrastructure Protection • Damage Control • Incident Response • Operational Security • Threat Hunters • Digital Forensics	• Combination of both Red and Blue • Facilitate improvements in detection and defense • Sharpened skills of Red and Blue team members • Effective for spot checking systems in larger organizations