**Ethical Hacking**

**PenTesting (Penetration testing) -> VAPT (Vulnerability Assessment and Penetration Testing)**

-> Web application PenTesting "Bug Bounty"

-> IOT

-> Mobile application (Android & iOS)

**Cloud Security**

**DevSecOps**

Hacking

Defensive

Offensive

**Triad (CIA/Pillars of Security)**

C - Confidentiality

I - Integrity

A - Availability

A - Authenticity

NR - Non-reputational

Confidentiality: In confidentiality, data exchange between two people is not accessible to the third person.

Integrity: In integrity, data exchange between two people should not be tampered.

Availability: At any given point of time, data should be accessible to its legitimate user.

Authenticity: Before providing the data, the system has to verify - Is the user same as he portrays?

Non-reputational: A person shouldn't be able to deny the activity he performed.

A person cannot deny his activity after performing it.

**Data states**

1. Data in Transit
2. Data in Use
3. Data at Rest
4. Data in Transit - When the data is moving
5. Data in Use - When the data is being processed
6. Data at Rest - When the data is not moving

OSIG (Open-Source Information Gathering)

**Hacking Phases**

1. Reconnaissance (Information Gathering)

Capturing information about the target

1. Extrapolation (Gaining access)
2. Privilege Escalation
3. Maintaining access

Creating a backdoor

1. Erase Traces

Clearing logs (Clearing footprints)

Cyber Killchain Methodology