Mini Project : Footprinting & Social Engineering Investigation

- Subtitle: *Ethical Hacking & Cybersecurity*
- Presented by: Daksh
- 2023A7R003
- Cse-CyberSecurity

Objective

Gather	Gather passive information about a test organization (OSINT)
Develop	Develop a social engineering exploit scenario (not executed)
Learn	Learn how attackers use reconnaissance to plan attacks

Key Topics

- **Footprinting** → Collecting info about targets
- **Social Engineering** → Tricking humans for access
- **OSINT (Open Source Intelligence)** → Publicly available info
- **Countermeasures** → Defensive strategies

Tools Used

- **Maltego** → Visualize relationships (domains, people, infra)
- **Shodan** → Find exposed devices & services
- **Google Dorks** → Search for hidden/sensitive data
- **LinkedIn** → Employee information & job roles

OSINT Report (Sample Findings)

- Domains & IPs of target
- Email addresses & employee info
- Open ports & technologies in use
- Social media profiles

Exploit Plan (Example Scenario)

- Target: HR Manager at test organization
- Exploit: Fake job application phishing email
- Payload: Malicious attachment (design only, not executed)
- Goal: Demonstrate how attackers could trick users

Defense Recommendations & Conclusion

- Employee security awareness training
- Limit public exposure of sensitive data
- Use email filtering & firewalls
- Conduct regular penetration tests & OSINT reviews
- *Outcome:* Learned attacker mindset & preventive measures