Assignment – 2

1) **Prepare a Case Study on the shortage of cybersecurity professionals in India, its impact on organizations, and the measures needed to address this challenge (Discuss the specific implications for the Indian context)**

Ans:

Case Study: Cybersecurity Skills Shortage in India

Problem:

- High demand, low supply of cybersecurity professionals.
- Global challenge, but India's gap is significant.

Impact:

- Increased vulnerability, slow response times, compliance challenges.

Unique Challenges in India:

- Skills gap between education and industry needs.
- Soft skills deficit hinders incident response.
- Focus on degrees over practical experience.

Solutions:

- Government support for skill development.
- Industry collaboration to update curriculum.
- Upskilling programs for existing IT professionals.
- Promote cybersecurity careers to a wider talent pool.
- Leverage AI/automation for streamlined tasks

2) **Analyse a significant cyber-attack(s) that has affected an Indian organization or institution. Evaluate the specific challenges faced, the response to the incident, and the lesson learned.**

Ans:

Case Study: Cyberattack on Oil India Limited (April 2022)

Attack:

- **Target:** Oil India Limited (OIL), a state-run oil and gas company.
- **Type:** Ransomware attack.
- **Attackers:** Unknown.

Challenges Faced:

- **Disruption, Data Breach, Financial Loss, Reputational Damage:** The attack caused operational disruption, potential data breaches, financial losses due to ransom demands, and reputational harm.

Response:

- **Limited Public Information:** Details on OIL's response are scarce.
- **Focus on Restoration:** Reports suggest OIL prioritized restoring systems.

Lessons Learned:

- **Stronger Defences, Training, Response Plans:** The attack highlights the need for robust cybersecurity measures, employee training, and incident response plans.
- **Transparency is Key:** Clear communication during and after an attack is essential.

Indian Context:

- **Critical Infrastructure Vulnerability:** This attack exposes the vulnerability of India's critical infrastructure to cyberattacks.
- **Focus on Data Security:** India's data privacy regulations necessitate robust data security practices.
- **Need for Public-Private Collaboration:** Collaboration is essential for defense strategies.

3) Investigate the top cybersecurity problems faced by universities and colleges, with a focus on the specific types of cyberattacks targeting higher education institutions.

Ans:

Top Cybersecurity Problems in Indian Universities and Colleges

Universities and colleges in India face a complex cybersecurity landscape. Here's a breakdown of the top problems and the cyberattacks targeting them:

Large attack surface, data breaches, outdated systems, insider threats, and lack of awareness leave universities vulnerable to phishing, ransomware, malware, and unauthorized access.

Limited budgets, skills gaps, and third-party vendor risks exacerbate these challenges in the Indian context.

Universities need to:

- Invest in security and training.
- Develop incident response plans.
- Collaborate with cybersecurity experts.
- Update curriculum and evaluate vendors.

4) Select and analyse three real-world malware attacks, covering different malware types such as viruses, worms, and ransomware. For each case, describe the attack vector, the target, the impact.

Ans:

Real-World Malware Attacks: A Comparative Analysis

Here's a breakdown of three real-world malware attacks, highlighting the malware type, attack vector, target, and impact:

Attack	Malware	Vector	Target	Impact	
WannaCry	Ransomware	Exploit	Global Orgs	Encrypted data, disruption (billions $)	
ILOVEYOU	Worm	Phishing	Users	Data loss, crashes, disrupted email	
Stuxnet	Worm (Trojan/Rootkit)	USB/Software Vuln.	Iran Facilities	Damaged centrifuges (potential program delay)	

5) Provide Comparative Analysis on DES, AES, RSA.

Ans:

Category	DES	AES	RSA
Type	Symmetric	Symmetric	Asymmetric
Key	Single Secret Key	Single Secret Key	Public-Private Key Pair
Key Length	Weak (56 bits)	Strong (128, 192, 256 bits)	Long (1024 to 4096 bits)
Speed	Fast	Faster	Slower
Security	Insecure	Secure	Not ideal for bulk encryption

Applications	Legacy systems	Bulk encryption	Digital signatures, key exchange