1) What is ToR and discuss attacks that are possible on it. Install ToR on your system and compare and contrast it with a regular search engine like Google?

Answer:

Tor: The Onion Router

Tor is a free, open-source software that anonymizes your online traffic. It encrypts data in layers and routes it through a network of relays, hiding your origin and destination.

Attacks on Tor

While Tor offers anonymity, it's not fool proof. Here are potential vulnerabilities:

- **Exit node attacks:** Malicious actors might compromise exit nodes, potentially intercepting unencrypted traffic leaving the Tor network.
- **Traffic analysis:** Advanced techniques can analyse traffic patterns to identify Tor users and potentially de-anonymize them.
- **Zero-day attacks:** Exploiting unknown vulnerabilities in Tor software could compromise user anonymity.

Feature	Tor Browser	Regular Search Engine (Google)
Anonymity	High	Low
Privacy	Encrypts traffic, hides browsing activity	Tracks user data, personalizes search
Speed	Slower due to multi-hop routing	Faster
Security	Protects from basic tracking, some vulnerabilities	More secure for financial transactions
Access to Websites	Accesses onion sites (dark web)	Limited access to specific websites
Legality	Legal for browsing but not illegal activities	Legal use

2) Use the web site http://testphp.vulnweb.com/ for the following. Perform sql injection on it and retrieve the user table and its contents.

Answer:

Risk & Legality: SQLi attacks can be risky and illegal. Even on a test site, practicing them could introduce vulnerabilities.

Learn Safely:

Virtual Labs: Practice in safe, controlled environments.

Courses: Learn SQLi concepts and mitigation strategies ethically.

3) What are Deepfakes? Discuss how they are being used for Impersonation attacks. Explain how they can be countered.

Answer:

deepfakes can be used for impersonation attacks:

- **Fake news:** Sway public opinion with fabricated political videos.
- **Financial scams:** Trick employees into fraud with deepfake CEOs.
- **Social engineering:** Manipulate people with deepfakes of friends or celebrities.
- **Reputation damage:** Deepfakes can be used to create compromising videos.

Countering deepfakes is an ongoing effort: better detection, public awareness, digital watermarking, and regulation.

4) Discuss about different types of Cyber crimes. Explain how a person can report to the concerned officials and take protection

Answer:

Cyber Crimes: Understanding the Threats and Taking Action

The digital world offers vast opportunities, but it also harbors a dark side: cybercrime. Here's a breakdown of common cyber crimes and how to report and protect yourself:

Cyber Crimes:

- Steal money (phishing, identity theft)
- Disrupt operations (malware, DoS)
- Harass or bully (cyberstalking, cyberbullying)
- Steal data (data breaches)

Report:

- Local law enforcement
- FBI's IC3 (https://www.ic3.gov/Home/ComplaintChoice)
- FTC (identity theft)

Protect Yourself:

- Strong passwords & 2FA
- Update software
- Beware of phishing
- Antivirus & anti-malware
- Back up data
- Secure browsing
- Stay informed (DHS CISA, NIST)

5) Discuss about various online payment frauds and how can they be prevented?

Answer:

Online Payment Fraud: Threats and Safeguards

Online payments offer convenience, but they also attract fraudsters. Here's a breakdown of common online payment scams and how to stay safe:

Types of Online Payment Fraud:

- **Identity Theft:** Criminals steal your card details (skimming, data breaches) and use them for online purchases.
- **Phishing:** Deceptive emails or messages trick you into revealing financial information.
- **Friendly Fraud:** A customer claims they never received an item after already receiving it.
- **Card Not Present Fraud:** Fraudsters use stolen card details for online transactions without needing the physical card.
- **Account Takeover:** Hackers gain access to your online accounts and make unauthorized purchases.

Preventing Online Payment Fraud:

- **Secure Sites & Strong Passwords:** Use https:// and strong passwords with MFA.
- **Beware of Phishing:** Don't click suspicious links and monitor accounts.

- **Secure Payments:** Use secure platforms and consider virtual card numbers.
- **Public Wi-Fi with Caution:** Avoid online transactions on unsecured Wi-Fi.
- **Report Fraud:** Notify your bank if you suspect fraud.
- **Stay Informed & Update Software:** Keep informed and update software regularly.