CYBER SECURITY

ASSIGNMENT -13

NAME:B.Shanmukh

Reg.no: 282023-024

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.

ANS:

Understanding ToR (The Onion Router)

ToR is a privacy-focused network that anonymizes users' internet activity by routing traffic through multiple volunteer-operated servers (nodes). This process obscures the user's location and usage from surveillance and traffic analysis.

Possible Attacks on ToR

1. **Traffic Analysis**: Observing patterns in traffic entering and exiting the network to correlate activity.
2. **End-to-End Timing Attacks**: Correlating the timing of traffic entering and exiting the network to de-anonymize users.
3. **Sybil Attack**: Inserting multiple malicious nodes to control a significant portion of the network.
4. **Exit Node Eavesdropping**: Malicious exit nodes can read unencrypted traffic leaving the ToR network.

Installing ToR and Comparison with Google

1. **Installation:**
   - Download and install the ToR Browser from Tor Project's website.
   - Follow the setup instructions to configure and start using the ToR Browser.
2. **Comparison with Google**

Feature	TOR	GOOGLE
Privacy	High anonymity, routes traffic through multiple nodes.	Lower privacy, tracks user data for personalization.
Speed	Generally slower due to multiple relays.	Faster, optimized for speed and efficiency.
Access	Can access .onion sites (dark web).	Accesses the surface web.
Tracking	No tracking of user activity.	Extensive tracking for advertising and analytics.
Search Results	Limited to public web and dark web content.	Comprehensive indexing of the surface web.

- ToR provides enhanced privacy but with slower speeds and limited search capabilities, while Google offers extensive search capabilities and speed but at the cost of user privacy.

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.

ANS:

This article is based on our **previous** article where you have learned different techniques to perform SQL injection manually using dhakkan. Today we are again performing SQL injection manually on a live website “**vulnweb.com**” in order to reduce your stress of installing setup of dhakkan.

By performing sql injection we can retrieve the user table and its contents. The user table is as shown:

```
Table 1: artist
Table 2: Carts
Table 3: Categ
Table 4: Featured
Table 5: Guestbook
Table 6: Pictures
Table 7: Product
Table 8: users
```

Maybe we can get some important data from the **users** table, so let’s penetrate more inside. Again Use the concat function for table users for retrieving its entire column names.

We successfully retrieve all eight column names from inside the table users.

Then I have chosen only four columns i.e. **uname, pass, email** and **cc** for further enumeration.

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

ANS:

Deepfakes are synthetic media generated using artificial intelligence (AI) techniques, particularly deep learning algorithms. These techniques can manipulate and superimpose images, video, or audio onto existing content, creating highly convincing fake videos or audio recordings of individuals saying or doing things they never actually did.

Impersonation attacks using deepfakes involve creating fake videos or audio recordings of individuals, often public figures or high-profile individuals, with the intent to deceive viewers or listeners. These deepfake impersonations can be used for various malicious purposes:

1. **Misinformation and Disinformation**: Deepfake videos can be used to spread false information or propaganda by making it seem like a public figure is endorsing a particular viewpoint or making controversial statements they never actually made.

2. **Fraud and Scams**: Deepfakes can be used in fraud schemes, such as creating fake videos of CEOs or other executives instructing employees to transfer funds or disclose sensitive information.

3. **Blackmail and Extortion**: Deepfake videos can be used to create compromising situations, such as videos of individuals engaging in inappropriate behavior, which can then be used for blackmail or extortion.

Countermeasures against deepfake impersonation attacks include:

1. **Detection Algorithms**: Developing algorithms and tools capable of detecting deepfake content by analyzing inconsistencies in facial expressions, lip movements, and audio-visual discrepancies.

2. **Digital Watermarking**: Embedding digital watermarks or cryptographic signatures into media content during creation to verify its authenticity and detect any alterations.

3. **Media Forensics Tools**: Using specialized forensic tools to analyze and verify the authenticity of media content, including deepfake detection techniques.

4. **Education and Awareness**: Raising awareness among the public and media professionals about the existence and potential impact of deepfakes to encourage skepticism and critical thinking when consuming media content.

5. **Regulation and Policy**: Implementing laws and regulations to address the creation and distribution of deepfake content, including penalties for malicious use.

6. **Authentication Methods**: Implementing multi-factor authentication and other verification methods for sensitive transactions or communications to reduce the risk of impersonation attacks.

   While these countermeasures can help mitigate the impact of deepfake impersonation attacks, it's an ongoing challenge as deepfake technology continues to evolve, requiring constant adaptation and innovation in defense strategies.

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

ANS:

Cybercrime encompasses a wide range of illegal activities conducted using computer systems, networks, or digital devices. Here are some common types of cybercrimes:

1. **Identity Theft**: Theft of personal information, such as social security numbers, credit card numbers, or passwords, to impersonate individuals or commit fraud.

2. **Phishing**: Sending fraudulent emails, messages, or websites that mimic legitimate ones to trick individuals into revealing sensitive information or downloading malware.

3. **Malware**: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or networks, including viruses, worms, Trojans, and ransomware.

4. **Cyberbullying**: Harassment, intimidation, or humiliation of individuals using digital communication tools, such as social media, email, or messaging apps.

5. **Online Scams**: Various fraudulent schemes conducted online, such as romance scams, investment scams, lottery scams, and fake charity scams, aimed at deceiving victims for financial gain.

6. **Data Breaches**: Unauthorized access to and theft of sensitive data from organizations or individuals, often resulting in the exposure of personal or financial information.

7. **Cyber Espionage**: Illegally accessing and stealing confidential information from government agencies, corporations, or individuals for espionage or competitive advantage.

8. **Hacking**: Unauthorized access to computer systems or networks to steal, manipulate, or delete data, disrupt services, or gain control over systems.

9. **Distributed Denial of Service (DDoS) Attacks**: Overwhelming a computer system, network, or website with a flood of traffic to disrupt its normal functioning and deny access to legitimate users.

10. **Child Exploitation**: Using the internet to exploit children for sexual purposes, including online grooming, distribution of child pornography, or solicitation of minors.

Reporting Cybercrimes and Taking Protection:

1. **Report to Law Enforcement**: Victims of cybercrimes can report incidents to local law enforcement agencies, cybercrime divisions, or specialized units such as the FBI's Internet Crime Complaint Center (IC3) in the United States.

2. **Use Reporting Platforms**: Many countries have dedicated online platforms or hotlines for reporting cybercrimes, where victims can submit complaints and seek assistance.

3. **Contact Financial Institutions**: In case of financial fraud or identity theft, victims should immediately contact their banks or credit card companies to report unauthorized transactions and request assistance.

4. **Document Evidence**: Victims should preserve any evidence related to the cybercrime, including emails, messages, transaction records, or screenshots, as it may be useful for investigations.

5. **Update Security Measures**: Individuals should regularly update their software, operating systems, and antivirus programs to protect against known vulnerabilities and malware threats.

6. **Use Strong Passwords**: Create strong, unique passwords for online accounts and enable two-factor authentication whenever possible to add an extra layer of security.

7. **Educate Yourself**: Stay informed about common cyber threats and scams, and educate yourself about safe online practices to avoid becoming a victim of cybercrime.

8. **Secure Privacy Settings**: Review and adjust privacy settings on social media accounts and other online platforms to control who can access your personal information.

- By taking proactive measures to protect themselves and promptly reporting any incidents of cybercrime, individuals can help law enforcement agencies investigate and prosecute offenders, as well as prevent further harm to themselves and others.

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

ANS:

Online payment frauds encompass a variety of schemes aimed at illegally obtaining money or financial information during online transactions. Here are some common types of online payment frauds and preventive measures:

1. **Phishing**: In phishing scams, fraudsters send deceptive emails or messages pretending to be from legitimate organizations, such as banks or e-commerce websites, to trick recipients into disclosing personal or financial information. Prevention:

- Be cautious of unsolicited emails or messages requesting sensitive information.
- Verify the legitimacy of websites and organizations before entering any personal or financial details.
- Use security tools like email filters and anti-phishing software to detect and block suspicious emails.

2. **Card Not Present (CNP) Fraud**: CNP fraud occurs when a fraudster uses stolen credit card information to make online purchases without physically presenting the card. Prevention:

- Implement multi-factor authentication for online transactions, such as requiring a one-time password or biometric verification.
- Use Address Verification Service (AVS) to match the billing address provided during the transaction with the one on file with the card issuer.
- Employ fraud detection tools that analyze transaction patterns and flag suspicious activity.

3. **Account Takeover (ATO)**: In ATO attacks, fraudsters gain unauthorized access to a user's online account, often by stealing login credentials through phishing or malware. Prevention:

- Use strong, unique passwords for each online account and enable two-factor authentication whenever possible.
- Regularly monitor account activity for any unauthorized transactions or changes.
- Educate users about the importance of password security and phishing awareness.

4. **Friendly Fraud**: Friendly fraud occurs when a legitimate account holder disputes a transaction, claiming it was unauthorized, even though they made the purchase. Prevention:

- Maintain detailed transaction records and documentation to provide evidence in case of disputes.
- Implement policies and procedures for handling disputes and chargebacks in a timely manner.
- Educate customers about the consequences of filing false claims and the impact on merchants.

5. **Identity Theft**: Identity theft involves stealing personal information, such as social security numbers or driver's license numbers, to fraudulently open accounts or make purchases in someone else's name. Prevention:

- Secure personal information by using encrypted connections and trusted websites for online transactions.
- Regularly monitor credit reports and financial statements for any suspicious activity.
- Consider using identity theft protection services that monitor for signs of identity theft and provide assistance in case of a breach.

6. **Card Skimming**: Card skimming involves installing devices on ATMs or point-of-sale terminals to capture credit or debit card information during transactions. Prevention:

- Inspect ATMs and card readers for any signs of tampering before use.
- Use contactless payment methods, such as mobile wallets or chip cards, to minimize the risk of card skimming.
- Monitor bank statements for unauthorized transactions and report any suspicious activity to the card issuer.

Preventing online payment fraud requires a combination of technological solutions, security protocols, and user awareness. By implementing proactive measures and staying vigilant against emerging threats, both merchants and consumers can reduce the risk of falling victim to online payment frauds.