ASSIGNMENT -13

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:

The attack tricks a user's web browser into sending a distinctive signal over the Tor network that can be detected using traffic analysis. It is delivered by a malicious exit node using a man-in-the- middle attack on HTTP. Both the attack and the traffic analysis can be performed by an adversary with limited resources.

Tor (an acronym for The Onion Router) is essentially a network that masks online traffic. Tor browser is an open-source platform managed by volunteers and, due to its onion routing, creates anonymity for users who access websites and servers through this network.

1. User Behavior Analysis:

This attack targets the traffic between Tor's Exit node and the destination site. The exit node is the node that communicates to the destination site on the internet. This is the point where all the Tor traffic will come out of the Tor network to join with other internet traffic. This gives a great opportunity for government agencies to de-anonymize Tor users. This technique just works by monitoring and analyzing the traffic of anonymized users leaving Tor exit nodes and correlating the traffic with available information.

2. Passive Traffic Analysis:

Passive Traffic analysis is quite similar to User Behavior analysis. Both analysis techniques will try to tie the Tor and regular internet traffic to de-anonymize Tor users. Then, you may ask what makes Passive Traffic analysis different from the User Behavior analysis attack. User Behavior analysis depends on the insecure activities of the users, where Passive Traffic analysis looks for the patterns of a computer, browser, and network.

3. Circuit Reconstruction:

It's not a secret that the Tor network creates a virtual circuit by selecting random nodes. The idea behind this attack is to reconstruct the circuit between entry and exit nodes. If it had been possible to reconstruct the circuit, it would not have remained private and anonymous. This attack is directly targeting the perfect forward secrecy, which is the core tech behind the Tor network. Please read the "What does happen inside the Tor network?" post to understand how the Tor network operates.

4. Circuit Shaping:

A successful Circuit Reconstruction attack needs a large number of compromised or owned nodes. What if an attacker can control the Victim's circuit with a small number of compromised nodes? In the Circuit Shaping attack, the attacker compromises the Victim's computer or Tor browser and modifies the Tor browser to only use the compromised nodes instead of random nodes. Circuit Shaping attack needs two things primarily. Either attacker should have access to the Victim's computer and alter the Tor. Or, the attacker forces the user to download and install the modified version of Tor.

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:

1. Open the website and click the signup button you will get the Login page and like I said before it is vulnerable website and SQL vulnerability already exist in this application.
2. After getting Login Page just do login with any credential and Capture the Request in Burp suite.
3. Now we need to save this POST request in file, to do this we have an option "**COPY to FILE**" in burp.
4. After Copying to file, Move that copied the file into Kali Linux machine. if you're using **Kali Linux App** in **Windows 11** then no need to move the file you can directly use the file, but I'm using Kali Linux in the Virtual box so I moved that file there
5. Now run the SQLMAP tool directly or using command "**SQLmap**", After running the tool give the below command and hit enter.
6. You can see if it is vulnerable to SQL injection. it will exploit automatically and it will give you the database details.
7. Successfully we got a databases. now we can retrieve what are the Tables present in the database by using the following command.
8. We successfully retrieved the "**Tables**" now we going to retrieve the "**columns**" from that databases.
9. Finally we have retrieved all data from that database, SQLmap out put will be saved in default location.

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

ANS:

Deepfake is the use of machine ("*deep*") learning to produce a kind of fake media content – typically a video with or without audio – that has been 'doctored' or fabricated to make it appear that some person or persons did or said something that in fact they did not.

Deepfake is a technology that creates convincingly **fictional** videos or photos of people from scratch. It basically uses deep learning AI to replace the face of one person with another in videos and other digital media.

Current cutting-edge deepfake AI is powered by two machine learning models working against each other. The "generator" algorithm is trained using sample imagery, audio, and/or video to create a new piece of media – or manipulate an existing one – that collectively resembles the samples as closely as possible.

The "discriminator" algorithm, meanwhile, is trained to recognize distinctive features in the samples, and point out where the "generator" misses them so it can go back and correct those inconsistencies.

This is known as a generative adversarial network, or GAN. Basically, it works like this:

1. The generator and discriminator algorithms analyze data from media samples.
2. The generator creates (or manipulates) media to collectively resemble the samples as nearly as it can. This is the initial deepfake.
3. The discriminator checks for inconsistencies between the samples and the deepfake.
4. The generator fixes inconsistencies the discriminator finds in the deepfake, and resubmits the deepfake to the discriminator.
5. Steps 3 and 4 repeat until the discriminator can find no more inconsistencies.

This process allows the generator to eventually create or manipulate media so accurately that neither artificial intelligence nor human intelligence can easily tell the difference between a deepfake and the genuine media it’s based on.

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

ANS:

TYPES OF CRIMES

Email Scams

Misleading schemes that take many forms. Fake emails mislead recipients, while social engineering techniques deceive people into divulging information, such as credit card numbers, or transferring money to the attacker. Phishing schemes, whereby scammers mimic legitimate brands, are a common form of email scams.

Social Media Fraud

Scams that use social media platforms like Facebook, Twitter, Instagram, and TikTok to deceive and defraud victims. Examples include fictitious online stores, catfishing, social engineering attacks, or impersonation scams. Social media frauds often exploit user trust, naivety, and a tendency to overshare personal information online.

Banking Fraud

Fraudulent activities that target financial institutions or their customers and stakeholders. Banking frauds most commonly result in significant financial loss or identity theft, and attacker strategies often involve sophisticated hacking and social engineering tactics. Examples include credit card fraud, ATM skimming, and online banking scams.

eCommerce Fraud

Elaborate consumer scams that exploit weaknesses and pitfalls of online shopping technologies, like artificial or fabricated online stores, fake seller accounts, or credit card information theft. Cases of eCommerce fraud typically result in financial losses on behalf of both consumers and online retailers.

Malware

A highly-prevalent software attack programmed to damage and manipulate computer systems by introducing viruses, trojans, or spyware into the system. Malware is a frequent problem across many cases because it targets both individual PCs and enterprise-level computer networks. It's most commonly used for disrupting networks and stealing data from users.

Ransomware

A type of malware attack that encrypts victims' critical data and declares a ransom payment in exchange for a decryption key to recover access. Financially crippling for individuals and organizations alike, ransomware attacks often lead to data and asset loss, fiscal devastation, and disrupted productivity. One of the most talked about ransomware cases involved Costa Rica's government and erupted into a national emergency.

Cyber Espionage

The use of hacking, malware attacks, or other cyber activity in which an unauthorized user attempts to access sensitive data or intellectual property to gain a competitive advantage over a company or government entity. Cases of cyber espionage often involve state-sponsored groups or individual hackers and can have

major political or economic implications. One of the most significant cases of cyber espionage was the five Chinese military hackers indicted for computer hacking, economic espionage, and other offenses directed at U.S. entities.

Data Breaches

Unauthorized access or leaks of sensitive data, such as confidential information, critical records, or financial access. Data breaches can be attributed to a wide array of risk factors, such as weak passwords and cybersecurity protocols, software system vulnerabilities, or insider threats. The consequences can result in compromised data, financial damages, or tarnished reputations. Verizon's data breach investigations report highlighted that 82% of breaches involved a human element.

Computer Viruses

Perhaps the most common type of malicious software that can self-replicate and spread to other systems, often causing damage to computer files or programs. Examples of computer viruses include the Melissa, ILOVEYOU, and Nimda viruses - all spread fast to infect files and damage computer systems.

DDoS Attacks

Distributed Denial of Service attacks, or DDoS attacks, are programmed to overwhelm a network or website with traffic, causing it to slow down or crash entirely. DDoS attacks were one of many of Russia’s destructive cyber activities against Ukraine, along with other attacks designed to delete computer data belonging to governmental and private entities.

Software Piracy

A digital form of intellectual property theft involving unauthorized use or distribution of copyrighted material, such as software, music, or movies. Examples of software piracy include using key generators or crack software to activate paid software without a license.

Phishing Scams

Email fraud that involves techniques like deceptive emails, website scams, or misleading communications to con victims into sharing their personal information and sensitive data or clicking links to malicious downloads and websites. Examples of phishing scams involve emails that appear to be from household brands, financial institutions, government agencies, or social media sites.

Identity Theft

In a digital context, identity theft refers to acquiring someone's private data for fraudulent or malicious purposes. Target assets of identity theft include social security numbers, date of birth, credit card details, or online accounts. Specific types include financial, medical, and tax identity theft; social media impersonation; and identity cloning, when a person uses another's identity to conceal their own.

Online Harassment

Involves cyberbullying, cyberstalking, and repeated acts intended to scare, harm, anger, or shame a particular individual. Today, online harassment is most prevalent on social media sites, dating apps, and forums/message boards. Examples of online harassment include sending inappropriate and unsolicited messages, making clear and intentional threats, or distributing sensitive photos or videos of a victim.

Cyber Terrorism

Generally grander acts of destruction online by using the Internet or computer technology to carry out acts of terror, such as causing infrastructure damage and catastrophic malfunctions, stealing confidential information, or spreading propaganda with political or cultural implications. Cases of cyber terrorism are becoming increasingly sophisticated, placing higher demands on cybersecurity and protection.

1. **Unauthorized Access and Hacking:**

   Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are the most targeted sites for the hackers.

   2. Web Hijacking:

   Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

3. Pornography:

Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.

4. Child Pornography:

The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cyber crime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet.

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

ANS:

1. Phishing

Phishing involves fraudsters impersonating legitimate organizations via email, text messages, or social media to steal sensitive data. These messages often contain links to fake websites where unsuspecting victims enter personal information.

2. Identity Theft

Identity theft occurs when fraudsters obtain enough personal information to impersonate individuals and gain access to their financial accounts, apply for loans, or make purchases. This data can be sourced through data breaches, phishing, or malware.

3. Payment Fraud

This includes any fraudulent transaction where a fraudster uses stolen payment card details to make unauthorized purchases or withdrawals. It often involves credit card skimming, data breaches, or intercepting online transactions.

4. Advance-Fee Fraud

Victims are persuaded to make advance payments for goods, services, or benefits that do not materialize. Common examples include lottery scams and job offer scams, where victims pay upfront fees for opportunities that are fictitious.

5. Investment Fraud

These scams involve the promotion of fake investment opportunities, enticing victims with the promise of high returns. Ponzi schemes and pyramid schemes are typical examples of investment fraud.

6. Ransomware and Malware

Malware, including ransomware, is used to gain unauthorized access to a victim's computer. Once installed, it can lock a user’s files (ransomware) or log keystrokes to steal credentials (spyware).

7. Romance Scams

Fraudsters create fake profiles on dating sites or social media platforms to manipulate and steal money from individuals looking for romantic partners. These scams often involve long-term deceit to build trust before asking for money.

8. Business Email Compromise (BEC)

In BEC scams, fraudsters target companies with emails that mimic communications from executives or high-level employees. The objective is to deceive staff into transferring money or sensitive information to the scammer’s accounts.

How to Protect Against Online Fraud

1. Educate and Train Staff and Clients

Awareness is the first line of defense against fraud. Regular training sessions for employees on recognizing phishing attempts, suspicious activities, and security protocols are essential. Similarly, educating clients on the risks and signs of fraud can empower them to be vigilant.

2. Implement Strong Authentication Processes

Strong authentication mechanisms such as two-factor authentication (2FA), biometric verification, and complex password requirements can significantly reduce the risk of unauthorized access to accounts and sensitive information.

3. Use Advanced Fraud Detection Systems

Investing in advanced fraud detection technologies that utilize machine learning and artificial intelligence can help identify and block fraudulent activities before they cause harm. These systems learn from patterns of normal and suspicious behaviors to improve their detection capabilities over time.

4. Secure and Monitor Networks

Ensuring that all network connections are secure, using encryption for data transmission, and employing firewalls and antivirus software are crucial in protecting against cyber threats. Continuous monitoring of network activities can also quickly uncover any unusual or potentially fraudulent actions.

5. Maintain Up-to-Date Software

Cyber threats evolve rapidly, and so must our defenses. Regularly updating software, operating systems, and applications with the latest security patches can close vulnerabilities that could be exploited by fraudsters.

6. Develop Comprehensive Incident Response Plans

Having a well-defined incident response plan ensures that an organization can react swiftly and effectively in the event of a fraud incident. This plan should include procedures for isolating affected systems, conducting forensic investigations, and notifying affected clients and authorities.

7. Leverage Information Sharing Platforms

Participating in forums and networks where organizations share information about fraud trends and attacks can provide early warnings about new types of fraud and effective prevention strategies.

8. Regular Audits and Compliance Checks

Regular audits of financial and IT systems can help identify and mitigate vulnerabilities before they are exploited. Compliance checks ensure that all protective measures align with local and international AML regulations.