UNIT TEST QB ANSWERS

Question –Explain Various types of Threats in detail.

Answer–

1. Malware: Malware is a broad category encompassing malicious software like viruses, worms, adware, Trojan horses, and spyware. These pose a significant threat to your system. Viruses replicate and hide in programs, often spreading through email accounts. Trojan horses appear benign but secretly download malware, and spyware spies on user activities, sometimes recording browsing history.

Example: A virus spreads through an email attachment, infecting the recipient's computer and using their email account to propagate itself to others in the address book.

2. Security Breaches: Security breaches involve unauthorized attempts to access systems, encompassing activities such as password cracking, privilege elevation, and server break-ins. Commonly associated with hacking, these breaches aim to compromise system integrity.

Example: A hacker attempts to gain unauthorized access to a company server by cracking passwords, exploiting vulnerabilities, or elevating privileges, with the intention of compromising sensitive information.

3. Denial of Service (DoS) Attacks: DoS attacks are designed to disrupt legitimate access to a system. Attackers flood the targeted system with false connection requests, rendering it unresponsive to genuine requests. This is a prevalent type of web attack.

Example: A DoS attack overwhelms a website by flooding it with an excessive number of false connection requests, rendering it inaccessible to legitimate users.

4. Web Attacks: Web attacks target websites, exploiting vulnerabilities in user-interactive features. SQL injection is a common method, involving inputting SQL commands into login forms to manipulate servers and gain unauthorized access.

Example: An attacker uses SQL injection by entering malicious SQL commands into a website's login form, manipulating the server into granting unauthorized access to sensitive databases

5. Session Hijacking: Session hijacking is an advanced attack where an attacker takes over an authenticated session between a client machine and a server. Though complex, it can lead to unauthorized access.

Example: A sophisticated attacker monitors and intercepts an authenticated session between a user and a banking website, taking control of the session to perform unauthorized transactions.

6. DNS Poisoning: DNS poisoning compromises the Domain Name Service (DNS), redirecting traffic to malicious sites. This attack aims to steal personal information by manipulating the translation of domain names into IP addresses.

Example: Malicious actors manipulate DNS records to redirect traffic intended for a legitimate banking website to a fraudulent site, aiming to steal login credentials and personal information.

7. Social Engineering: Social engineering exploits human nature to breach system security. Attackers gather preliminary information about a target organization and use it to manipulate individuals into revealing sensitive information, such as usernames and passwords.

Example: An attacker, armed with information about a target organization, calls an employee claiming to be from the IT department and convinces them to reveal their username and password.

8. War-Driving: War-driving is a form of attack associated with wireless networks. Attackers drive around locating vulnerable wireless networks, taking advantage of signals extending beyond physical boundaries.

Example: A hacker drives around a city scanning for vulnerable wireless networks, exploiting the fact that wireless signals often extend beyond physical boundaries, gaining unauthorized access to poorly secured networks.

9. Logic Bombs: Logic bombs are dormant software activated under specific conditions, often a set date and time. Once triggered, they execute malicious actions like deleting files or releasing viruses.

Example: A disgruntled employee installs a logic bomb in the company's system set to activate on a specific date, causing data loss and disruption to operations as an act of revenge.

Question – what is the virus explain with the example

Answer–

Definition: A computer virus is a self-replicating program that can spread from one computer to another, often with an accompanying payload that may harm the system or disrupt its normal functionality. The key characteristics of a virus include self-replication and rapid spread, with the potential to cause harm to the infected system.

How a Virus Spreads:

1. **Network Scanning:** A virus scans a computer for network connections and copies itself to other machines on the network.
2. **Email Propagation:** A common method is to read the email address book and email itself to everyone in the address book. This method is often exploited due to its simplicity.

Example: *Imagine receiving an email with a subject like "Important Document" or "Check this Out!" The virus, attached to the email, spreads by enticing users to open the attachment. Once opened, the virus replicates and may execute harmful actions on the infected system.*

Recent Virus Examples:

1. **W32/Netsky-P (2006 - 2011):**
    - Spreads through email and file-sharing utilities.
    - Attempts to disguise itself by using names like "FVProtect.exe" and "userconfig9x.dll."
2. **Troj/Invo-Zip (2010):**
    - Transmitted as a zip file attached to an email, often related to invoices or tax issues.
    - Installs spyware on the machine, disabling the firewall and capturing sensitive information.
3. **MacDefender (2011):**

- Targets Macintosh computers, taking advantage of the growing market share of Apple products.
- Tricks users into downloading a fake antivirus product by falsely claiming the presence of a virus.

4. **Sobig Virus (2003):**
    - Spreads via email and shared drives, utilizing multiple routes for propagation.
    - Generates significant network traffic, causing slowdowns but does not destroy files.
5. **Mimail Virus:**
    - Collects email addresses not only from the address book but also from other documents on the infected machine.
    - Utilizes its own built-in email engine, spreading independently of the user's email client.
6. **Bagle Virus (2003):**
    - Spreads through email attachments, often posing as communication from the system administrator.
    - Disables processes used by antivirus scanners, compromising the computer's "immune system."

Rules for Avoiding Viruses:

1. Use a reputable virus scanner like McAfee, Norton, Kaspersky, or AVG.
2. Avoid opening email attachments if unsure of their origin.
3. Establish a code word for attachments with friends and colleagues.
4. Be cautious of unsolicited security alerts and regularly check official websites for updates.

Question – what is the virus explain with the example

Answer–

Basic Cybersecurity Terminology

Understanding basic cybersecurity terminology is essential for navigating the world of computer security. These terms provide a foundation for further exploration, and additional terms will be introduced throughout the learning process.

Hacker Slang:

- **Hacker:** An expert on a particular system who seeks to learn more about it by understanding its weaknesses and flaws.
- **White Hat Hacker:** Ethical hackers who report system flaws to the vendor, often hired for penetration tests.
- **Black Hat Hacker (Cracker):** Gains unauthorized access to cause harm, steal data, or disrupt systems.
- **Gray Hat Hacker:** Engages in potentially illegal activities but may not have malicious intent.

Script Kiddies:

- **Script Kiddy:** Individuals with limited hacking expertise who use pre-made tools to exploit systems without deep understanding.

Ethical Hacking (Sneakers):

- **Sneaker:** Legally hired professional who assesses system vulnerabilities to enhance security.
- **Ethical Hacking:** Authorized hacking performed for assessing and improving system security.

Phreaking:

- **Phreaking:** Illegitimate actions to avoid paying for telecommunications services, often involving the compromise of telephone systems.

Professional Terms:

- **Firewall:** A protective barrier between a network and the outside world that filters incoming and outgoing traffic.
- **Proxy Server:** Used with firewalls to hide internal network IP addresses and present a single IP address to the outside world.
- **Intrusion Detection System (IDS):** Monitors network traffic for suspicious activities that may indicate an intrusion.

Security Activities:

- **Authentication:** Verifying credentials (e.g., username and password) to determine if a user or system is authorized to access a network resource.
- **Auditing:** Reviewing logs, records, and procedures to ensure they meet security standards.

Question – how to protect yourself from the cyber crime

Answer–

Protecting Against Investment Fraud:

1. **Choose Reputable Brokers:**
    - Invest only with well-known and reputable brokers.
2. **Be Skeptical of Unrealistic Returns:**
    - Avoid investments that seem too good to be true.
3. **Question Motives:**
    - Ask why someone is sharing an incredible investment opportunity with you, especially if they are a stranger.
4. **Understand Risks:**
    - Recognize that even legitimate investments involve risk; only invest money you can afford to lose.

Protecting Against Identity Theft:

1. **Limit Personal Information Sharing:**
    - Avoid providing unnecessary personal information online, especially to unknown individuals.
2. **Secure Document Disposal:**
    - Destroy documents containing personal information using a paper shredder before disposal.
3. **Regularly Check Credit:**
    - Utilize websites like www.consumerinfo.com to check your credit and beacon score regularly.
    - Unauthorized items on your credit report may indicate identity theft.
4. **Monitor Driving Records:**

- If your state provides online driving records, check them annually for any unauthorized infractions.
- Unexpected driving violations could signal identity theft.

Privacy Protection:

1. **Control Information Exposure:**
    - Restrict the amount of personal information you share online.
2. **Monitor Online Activities:**
    - Regularly check credit reports and driving records to detect unauthorized use of your identity.
3. **Anti-Spyware Software:**
    - Use anti-spyware software to prevent websites from collecting information without your knowledge.
    - Detailed information on this will be covered in a later chapter.
4. **Manage Cookies:**
    - Be cautious of cookies that store information about your online activities.
    - Utilize anti-spyware tools and adjust browser settings to control exposure and protect privacy.

Question - how the internet fraud actually works

Answer–

Internet fraud encompasses various schemes, and understanding common scams can help you avoid falling victim to fraudulent activities. Here are some insights into the workings of internet fraud:

Investment Offers:

1. **Nigerian Fraud Scheme:**
    - Unsolicited emails claim to be from a deceased Nigerian official, offering to transfer funds through your bank account.
    - Requests for advance payments for taxes and fees follow, resulting in financial loss for victims.
2. **General Principles to Identify Fraud:**
    - Evaluate the risk-taking perspective of the person making the offer.
    - Assess if the deal seems overly biased in your favor.
    - Consider how you would approach the deal if you were in the other person's position.

Investment Advice:

1. **Paid Stock Recommendations:**
    - Some online newsletters receive compensation to recommend specific stocks.
    - U.S. securities laws require disclosure of such payments, but not all newsletters comply.
    - Paid recommendations may compromise the objectivity of stock advice.
2. **Pump and Dump Scheme:**
    - Con artists artificially inflate the value of a virtually worthless stock.

- Tactics include spreading rumors on forums and chat rooms, creating a false sense of market demand.
- The fraudster sells the inflated stock for profit before its value drops back to reality.

3. **Avoiding Stock Scams (SEC Tips):**
    - Consider the credibility of the information source.
    - Independently verify claims and conduct thorough research on the company.
    - Beware of high-pressure tactics and be skeptical of deals that seem too good to be true.

Victim Psychology:

- Fraud often preys on victims' greed, promising substantial returns with minimal effort.
- A healthy dose of skepticism and avoiding decisions based solely on financial greed can help prevent falling victim to fraud.

Question - Explain three areas of the beading frauds in details.

Answer–

What is Auction Fraud?

Auction fraud refers to deceptive practices and scams that can occur during online auctions, undermining the integrity of the bidding and buying process. While online auctions, like those on platforms such as eBay, offer opportunities for users to find merchandise at competitive prices, they also pose risks related to fraudulent activities. The U.S. Federal Trade Commission (FTC) categorizes auction fraud into several forms:

1. **Failure to Send the Merchandise:**
    - In this clear-cut case of fraud, the seller fails to deliver the purchased item after receiving payment.
    - **Risk:** Buyers may lose their money, especially in organized fraud schemes where the seller disappears after collecting funds from multiple auctions.
2. **Sending Something of Lesser Value Than Advertised:**
    - Sellers misrepresent the item, advertising features or attributes that do not match the delivered product's actual value.
    - **Gray Area:** While sometimes it results from intentional deception, it can also occur due to the seller's overzealousness or lack of awareness regarding the product's true attributes.
3. **Failure to Deliver in a Timely Manner:**
    - Sellers do not fulfill their obligation to deliver the purchased item within a reasonable timeframe.
    - **Uncertainty:** Whether this constitutes fraud or inadequate customer service depends on the circumstances surrounding the delay.
4. **Failure to Disclose All Relevant Information:**

- Sellers withhold important details about the product or the terms of the sale, potentially misleading buyers.
- **Causes:** Lack of transparency can result from either intentional fraud or the seller's ignorance about the item's condition or specifications.

Three Areas of Auction Frauds Explained

Online auctions, while providing opportunities for great deals, can be susceptible to various forms of fraud. Here are three areas of auction fraud explained in detail:

1. **Shill Bidding:**

- **Definition:** Shill bidding involves fraudulent sellers (or their accomplices, known as "shills") artificially bidding on their items to drive up the price.
- **Operation:**
  - Perpetrators create fake identities to bid on their own items.
  - This inflates the bidding competition, making genuine bidders believe the item is in higher demand.
- **Detection Challenges:**
  - Difficult to detect as the identity of the fake bidders is concealed.
- **Preventive Measures:**
  - Bidders should establish a maximum bid before participating.
  - Exercise restraint and avoid exceeding the predetermined bid, ensuring protection against artificially inflated prices.

2. **Bid Shielding:**

- **Definition:** Bid shielding occurs when fraudulent buyers place very high bids to discourage competitors, retracting bids later to obtain the item at a lower price.
- **Prevention by Auction Sites:**

    - Auction platforms, like eBay, may revoke bidding privileges for users who retract bids after winning an auction.
- **Addressing the Issue:**
    - Transparent bidding practices and consequences for bid retractions discourage bid shielding.
    - Ensures fair competition among genuine bidders.

3. **Bid Siphoning:**

- **Definition:** Bid siphoning involves luring bidders off legitimate auction sites by offering the same item at a lower price on external sites.
- **Scheme Operation:**
    - Perpetrators advertise a legitimate item on the auction site but redirect potential buyers to fraudulent external sites.
- **Risks for Buyers:**
    - Buyers lose protections provided by the original auction site, such as insurance, feedback forms, or guarantees.
    - Increased susceptibility to various fraud schemes on external sites.

Question - what is the cyber stalking explain in the detail

Answer-

Understanding Cyber Stalking

Cyber stalking refers to the use of the Internet, email, or other electronic communication devices to engage in persistent, harassing, or threatening behavior towards another individual. While there is no universally accepted definition, the essence lies in the repetitive nature of the harassment, akin to traditional stalking, but manifested in the digital realm.

Cyber stalking is a significant and punishable offense that has evolved with the digital age. Understanding its legal implications and the severity of real cases is crucial in addressing and preventing online harassment. As technology advances, the legal landscape surrounding cyber stalking will likely continue to evolve to protect individuals in the digital realm.

Elements of Cyber Stalking: The U.S. Department of Justice outlines key aspects of cyber stalking, which include:

1. **Harassing or Threatening Behavior:**
    - *Nature:* Involves persistent actions like following a person online, appearing at their digital spaces, making threatening phone calls, leaving written messages, or vandalizing their online presence.
    - *Legal Implications:* Laws generally require a credible threat of violence against the victim, with some also extending to threats against the victim's immediate family.
2. **Implied Threats:**
    - *Definition:* The course of conduct doesn't always necessitate explicit threats; an implied threat can be sufficient for legal consideration.
    - *Example:* Annoying or menacing behavior that falls short of illegal stalking may still be taken seriously if it hints at a potential escalation.
3. **Jurisdictional Variability:**

- *Challenges:* Determining what constitutes a crime can vary based on factors like the content of electronic communication, frequency, prior relationships, and jurisdiction.
- *Example:* Ceaseless emailing after being requested to stop may or may not be deemed a crime based on these factors.

Real Cyber Stalking Cases: Examining actual cases sheds light on the severity of cyber stalking:

1. *Impersonation and Solicitation:* A perpetrator impersonated a woman online, soliciting her rape in chat rooms, leading to real-life threats at her doorstep. The offender faced charges under California's cyber stalking law.
2. *Anonymous Harassment:* A Massachusetts case involved systematic harassment using anonymous re-mailers, escalating to an attempt to extort sexual favors from a co-worker under threats of disclosing past activities.
3. *Graduate Student's Vendetta:* A graduate student terrorized five female students for over a year, sending violent and threatening emails. The crimes were committed due to perceived ridicule, showcasing the seriousness of online harassment.

Legal Framework:

- *Existing Laws:* Many states have specific laws against cyber stalking, while federal laws may also apply. Laws against traditional stalking can be extended to cover cyber stalking.
- *Identity Theft Laws:* Identity theft laws, both at the state and federal levels, can encompass cyber stalking cases involving impersonation and deception.