CS Module 2 QB Solutions

1. Explain the basic stages during an attack on the network? Explain.2,6,8.

Network attack incidents reveal that attackers are often very systematic in launching their attacks. The basic stages of an attack are described here to understand how an attacker can compromise a network here:

- Initial Uncovering Reconnaissance
- Network probe Scanning potential or weaker targets
- Crossing the line toward electronic crime (E-crime)
- Capturing the network
- Grab the data
- Covering tracks

Stages of an Attack

1. Initial Uncovering

Two steps are involved here. In the first step called as reconnaissance, the attacker gathers information, as much as possible, about the target by legitimate means searching the information about the target on the Internet by Googling social networking websites and people finder websites.

2. Network probe

At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a ping sweep of the network IP addresses is performed to seek out potential targets, and then a port scanning tool.

3. Crossing the line towardelectronic crime (E-crime)

Now the attacker is toward committing what is technically a computer crime. He/she does this by exploiting possible holes on the target system.

Stages of an Attack Contd...

4. Capturing the network

At this stage, the attacker attempts to own the network. The attacker gains a foothold in the internal network quickly and easily, by compromising low-priority target systems. The next step is to remove any evidence of the attack.

5. Grab the data

Now that the attacker has captured the network he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites from your network, causing a potentially expensive and embarrassing situation for an individual and/or for an organization.

6. Covering tracks

This is the last step in any cyber-attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.

2. Write a short notes on Proxy Servers and Anonymizer? What are the purpose of the proxy servers?

Proxy Servers and Anonymizers

Proxy server is a computer on a network which acts as an intermediary for connections with other computers on that network. The attacker first connects to a proxy server and establishes a connection with the target system through existing connection with proxy.

Listed are few websites where free proxy servers can be found:

1. http://www.proxy4free.com
2. http://www.publicproxyservers.com
3. http://www.proxz.com
4. http://www.anonymitychecker.com
5. http://www.surf24h.com

Anonymizers

An Anonymizers or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the users behalf, protecting personal information by hiding the source computers identifying information.

Listed are few websites where more information about Anonymizers can be found:

1. http://www.anonymizer.com
2. http://www.browzar.com
3. http://www.anonymize.net
4. http://www.anonymouse.ws
5. http://www.anonymousindex.com

Purpose a Proxy Server

1. Keep the systems behind the curtain (mainly for securityreasons).
2. Speed up access to a resource (through caching). It is usually used to cache the webpages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxyserver can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address.

Advantage

A proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be by different users, it is likely to be in the proxys cache memory, which will improve user response time.

3. Explain in detail about Password Cracking.

Password Cracking

Password is like a key to get an entry into computerized systems like a lock. Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.
The purposeof password cracking is as follows:
1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual Password Cracking

The attacker follows the following steps:

1. Find a valid user account such as an administrator or guest
2. Create a list of possible passwords
3. Rank the passwords from high to low probability
4. Key-in each passwor
5. Try again until a successful password is found.

Passwords can also be guessed

1. Blank (none)
2. The words like password, passcode and admin.
3. Series of letters from the qwerty keyboard, for example, qwerty, asdf or qwertyuiop.
4. Users name or login name.
5. Name of users friend/relative/pet.
6. Users birthplace or date of birth, or a relatives or a friends.
7. Users vehicle number, office number, residence number or mobile number.
8. Name of a celebrity who is considered to be an idol by the user.
9. Simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

4. What are the different types of attack in password cracking? Explain strong, weak and random passwords.

Types of Attacks

Online Attacks:

An attacker can create a script file (i.e., automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system. The most popular online attack is man-in-the middle (MITM) attack, also termed as bucket-brigade attack or sometimes Janus attack.

Offline Attacks:

Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used.

Strong, Weak and Random Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords.
Here are some of the examples of weak passwords:

1. Susan: Common personal name.
2. aaaa: repeated letters, can be guessed.
3. rover: common name for a pet, also a dictionary word.
4. abc123: can be easily guessed.
5. admin: can be easily guessed.
6. 1234: can be easily guessed.
7. QWERTY: a sequence of adjacent letters on many keyboards.
8. 12/3/75: date, possibly of personal importance.
9. nbusr123: probably a username, and if so, can be very easily guessed.

Some of the examples of Strong Passwords:

1.**Convert Dollar 100 to Euros:** Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.

2. **382465304H:** It is mix of numbers and a letter at the end, usually used on mass user accounts and such passwords can be generated randomly.
3. **4pRte!ai@3:** It is not a dictionary word; however it has cases of alpha along with numeric and punctuation characters.
4. **MoOoOfIn245679:** It is long with both alphabets and numerals.
5. **t3wahSetyeT4:** It is not a dictionary word; however, it has both alphabets and numerals.

Random Passwords

Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters.
Password Policies:

1. Passwords and user logon identities (IDs) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters.
3. There should be computer-controlled lists of prescribed password rules and periodic testing to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues.
5. Passwords shall be changed every 30/45 days or less.
6. User accounts should be frozen after five failed logon attempts.

5. What are Keyloggers? Explain different types of Keyloggers?

Keyloggers

Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.

Different Types of Keyloggers:

1. Software Keyloggers
2. Hardware Keyloggers
3. Antikeylogger

Software Keyloggers

Software keyloggers are software programs installed on the computer systems which usually arelocatedbetweenthe OS and the keyboard hardware, and everykeystroke is recorded.

1.SC-KeyLog PRO

It allows to secretly record computer user activities such as E-Mails, chat conversations, visited websites, clipboard usage, etc. in a protected log file.

2. Spytech SpyAgent Stealth

It provides a large variety of essential computer monitoring features as well as website and application filtering, chat blocking and remote delivery of logs via E-Mail or FTP.

Software Keyloggers Contd..

3. All in one Keylogger

It is an invisible keystrokes recorder and a spy software tool that registers every activity on the PC to encrypted logs.

1. Stealth Keylogger
2. Perfect Keylogger
3. KGB Spy
4. Spy Buddy
5. Elite Keylogger
6. CyberSpy
7. Powered Keylogger

Hardware Keyloggers

To install these keyloggers, physical access to the computer system is required. Hardware keyloggers are small hardware devices.
Listed are few websites where more information about hardware keyloggers can be found:

1. http://www.keyghost.com
2. http://www.keelog.com
3. http://www.keydevil.com
4. http://www.keykatcher.com

Antikeylogger 2 points, in which it overtakes antivirus

Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool. Visit http://www.anti-keyloggers.com for more information. Advantages of using Antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, Antikeylogger can detect installations of keylogger.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs..
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft (we will discuss it more in Chapter 5).
5. It secures E-Mail and instant messaging/chatting.

6. What are Spyware? Explain any five Spywares with their Features and Function.

Spywares

Spyware is a type of malware that is installed on computers which collects information about users without their knowledge.
The features and functions of such Spywares are beyond simple monitoring:

1. 007 Spy:
   - Capability of overriding antispy programs like ad-aware;
   - Record all websites url visited in internet;
   - Powerful keylogger engine to capture all passwords;
   - View logs remotely from anywhere at any time;
   - Export log report in html format to view it in the browser;
   - Automatically clean-up on outdated logs;
   - Password protection.

Spywares Contd..

2. Spector Pro:
   - Captures and reviews all chats and instant messages;
   - Captures E-Mails (read, sent and received);
   - Captures websites visited;
   - Captures activities performed on social networking sites such as MySpace and Facebook;
   - Enables to block any particular website and/or chatting with anyone;
   - Acts as a keylogger to capture every single keystroke (including usernames and passwords).

Spywares Contd..

3. eBlaster:

Besides keylogger and website watcher, it also records E-Mails sent and received, files uploaded/downloaded, logging users activities, record online searches, recording Myspace and Facebook activities and anyother program activity.

4. Remotespy:

Besides remote computer monitoring, silently and invisibly, it also monitors and records users PC without any need for physical access. Moreover, it records keystrokes (keylogger), screenshots, E-Mail, passwords, chats, instant messenger conversations and websites visited.

Spywares Contd..

5.Stealth Recorder Pro:

It is a new type of utility that enables to record a variety of sounds and transfer them automatically through Internet without being notified by original location or source.
It has following features:
   - Real-time mp3 recording via microphone, cd, line-in and stereo mixer as mp3, wma or wav formatted files.
   - Transferring via e-mail or ftp, the recorded files to a user-defined e-mail address or ftp automatically.
   - Controlling from a remote location.
   - Voice mail, records and sends the voice messages.

6. Stealth Website Logger:

It records all accessed websites and a detailed report can be available on a specified E-Mail address.

Spywares Contd..

It has following key Features:

- Monitor visited websites;
- Reports sent to an E-Mail address;
- Daily log;
- Global log for a specified period;
- Log deletion after a specified period;
- Hotkey and password protection;
- Not visible in add/remove programs or task manager.

7. **Flexispy:** It is a tool that can be installed on a cell/mobile phone. After installation, Flexispy secretly records coversation that happens on the phone and sends this information to a specified E-Mail address.
8. **Wiretap Professional:** It is an application for monitoring and capturing all activities on the system. It can capture the entire Internet activity. ftis spy software can monitor and record E-Mail, chat messages and websites visited. In addition, it helps in monitoring and recording of keystrokes, passwords entered and all documents, pictures and folders viewed.
9. **PC Phone Home:** It is a software that tracks and locates lost or stolen laptop and desktop computers. Every time a computer system on which PC Phone Home has been installed,

Explain in detail about Virus.

Computer virus is a program that can infect legitimate programs by modifying them to include a possibly evolved copy of itself. Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.

Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus;
2. Delete files inside the system into which viruses enter;
3. Scramble data on a hard disk;
4. Cause erratic screen behavior;
5. Halt the system (PC);
6. Just replicate themselves to propagate further harm.

Viruses Spread

- Through the internet,
- Through a stand-alonecomputer system and
- Through local networks.

Viruses Spread Through the Internet

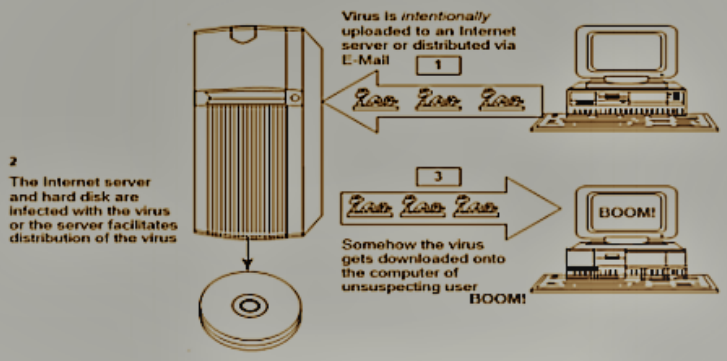


Fig: Virus spreads through the Internet.

Viruses Spread Through a stand-alonecomputer system

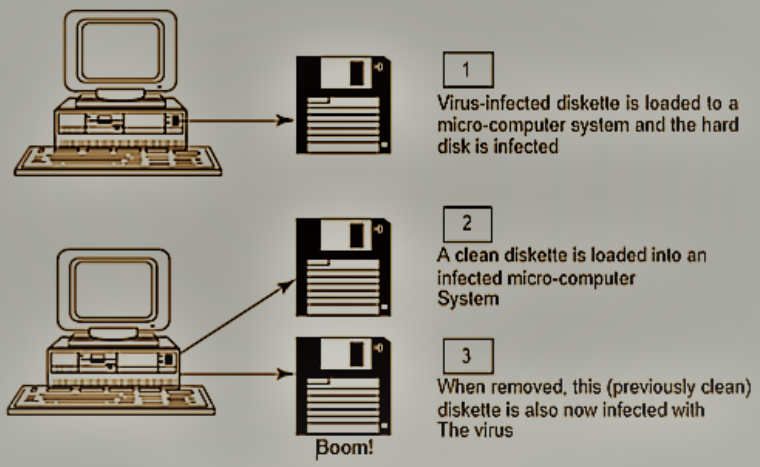


Fig: Virus spreads through stand-alone system.

Through local networks.

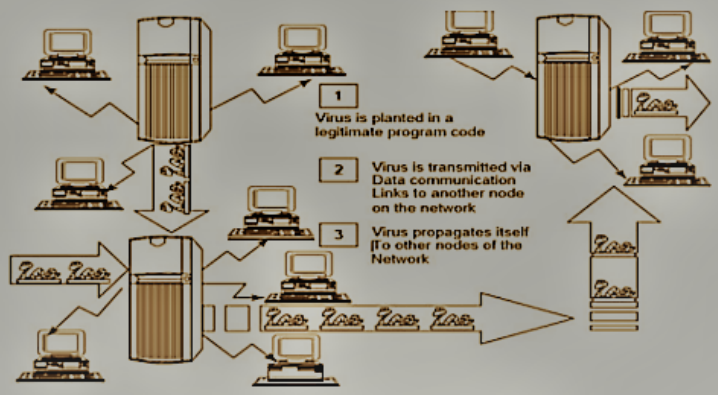


Fig: Virus spreads through local networks.

Types of Viruses

Computer viruses can be categorized based on attacks on various elements of the system and can put the system and personal data on the system in danger.

- Boot sector viruses
- Program viruses
- Multipartite viruses
- Stealth viruses
- Polymorphicviruses
- Macro viruses
- Active X and Java Control

7. What is the difference between Virus and Worms?

Difference between Virus and Worms

Difference between computer virus and worm

Sr. No.	Facet	Virus	Worm
1	Different types	Stealth virus, self-modified virus, Encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing networks worms
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software pro-Gram that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as The first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, *The Worm Programs* and after that the name was adopted
5	Prevalence	Over 100,000 known computer viruses Have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

8. Write a short on Trojan horse. List some of the threats by Trojan horse.

Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk. Some typical examples of threats by Trojans are as follows:

- They erase, overwrite or corrupt data on a computer.
- They help to spread other malware such as viruses (by a dropper Trojan).
- They deactivate or interfere with antivirus and firewall programs.
- They allow remote access to your computer (by a remote access Trojan).
- They upload and download files without your knowledge.
- They gather E-Mail addresses and use them for Spam.
- They log keystrokes to steal information such as passwords and credit card numbers.
- They copy fake links to false websites, display porno sites, play sounds/videos and display images.
- They slow down, restart or shutdown the system.
- They reinstall themselves after being disabled.
- They disable the task manager.
- They disable the control panel.

9. How to Protect the systems from Trojan Horses and Backdoors?

How to Protect from Trojan Horses and Backdoors

1. Stay away from suspect websites/weblinks: Avoid downloading free/pirated software's that often get infected by Trojans, worms, viruses and other things.
2. Surf on the Web cautiously: Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats.
3. It may be experienced that, after downloading the file, it never works and here is a threat that although the file has not worked, something must have happened to the system the malicious software deploys its gizmos and the system is at serious health risk.
4. Install antivirus/Trojan remover software: Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses.

10. What is backdoors? Explain some of the backdoor Trojans examples.

Backdoors

A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.

- They slow down, restart or shutdown the system.
- They reinstall themselves after being disabled.
- They disable the task manager.
- They disable the control panel.

Examples of Backdoor Trojans:

1. **Back Orifice:** It is a well-known example of backdoor Trojan designed for remote system administration. It enables a user to control a computer running the Microsoft Windows OS from a remote location. The name is a word play on Microsoft BackOffice Server software. Readers may visit http://www.cultdeadcow.com/tools/bo.html to know more about backdoor.
2. **Bifrost:** It is another backdoor Trojan that can infect Windows 95 through Vista. It uses the typical server, server builder and client backdoor program configuration to allow a remote attacker, who uses client, to execute arbitrary code on the compromised machine.
3. **SAP backdoors:** SAP is an Enterprise Resource Planning (ERP) system and nowadays ERP is the heart of the business technological platform. These systems handle the key business processes of the organization, such as procurement, invoicing, human resources management, billing, stock management and financial planning.
4. **Onapsis Bizploit:** It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs. Bizploit assists security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized ERP penetration tests. Readers may visit http://www.onapsis.com/research.html to know more about this tool.

11. What is the difference between Trojan horse and Backdoors?

Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk. Some typical examples of threats by Trojans are as follows:

They slow down, restart or shutdown the system. They reinstall themselves after being disabled.
They disable the task manager.
They disable the control panel.

Backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.

They slow down, restart or shutdown the system. They reinstall themselves after being disabled.
They disable the task manager.
They disable the control panel.

12. Write short notes on Steganography. Explain the classification of Steganography Techniques in detail

Stego means cover, graphymeans text/writing
* A plaintext message may be hidden in one of two ways.
* Steganography -conceals the existence of the message,
* cryptography -various transformations of the text.
* Steganography is data hidden within data.
* Along with cryptography as an extra-secure method to protect data.
* The technique of hiding information in any other information & also hiding the fact that communication is taking place is known as steganography.
* Steganography works by hiding information in a way that doesn't arouse suspicion. * One of the most popular techniques is 'least significant bit (LSB) steganography

Classification of Steganography Techniques:
– Spatial Domain Techniques:
• These techniques use the pixel gray levels and their color values directly for encoding the message bits.
• Simplest schemes in terms of embedding and extraction complexity.
• Least significant bit (lsb) replacement technique in which the lsb of the binary representation of the pixel gray levels is used to represent the message bit.
– Transform Domain Techniques:
• Try to encode message bits in the transform domain coefficients of the image.
• Watermarking.
• Discrete cosine transform (dct), discrete wavelet transform (dwt), and discrete fourier transform (dft).

13. What is the difference between Cryptography and Steganography?

Cryptography:
• An original message is known as plain text while the coded message is known as cipher text.
• The process of converting plain text to cipher text is known as ciphering or encryption, restoring the main text from cipher text is known as deciphering or decryption.
• The various schemes used for encryption are known as \Cryptographic system.
• Techniques used for deciphering are known as crypto-analysis.
• The area of cryptography and crypto-analysis together is called as cryptology.

Steganography:
• conceals the existence of message.
• The various techniques used are: – Character marking
– Invisible ink
– Pin
– Subset method

A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer system, network, or service, making it inaccessible to its intended users. The goal of a DoS attack is to overwhelm the targeted system's resources, such as bandwidth, processing power, or memory, to the point where legitimate users are unable to access or use the system.

14. Explain in detail about the DoS and DDos attack?

DoS and DDoS Attack
* A denial-of-service (dos) attack floods a with traffic, making a website or resource unavailable.
*A distributed denial-of-service (ddos) attack is a dos attack that uses multiple machines to flood a targeted resource
* Criminal act
* The attacker floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide.
* DOS attack only single device is used with DOS attack tools

* ddos attack bots are used to attack at the same time. Symptoms of dos attacks to include:
* unusually slow network performance (opening files or accessing websites);
* unavailability of a particular website;
* inability to access any website;
* dramatic increase in the number of spam e-mails receive of dos attack is termed as an e-mail bomb).

Goal of DOS
*Flood a network with traffic, thereby preventing legitimate network traffic. * Disrupt connections between two systems, thereby preventing access to a
service.
* Prevent a particular individual from accessing a service. * Disrupt service to a specific system or person.
Classification of DoS Attacks
1. Bandwidth Attacks:
2. Logic Attacks: ,
3. Protocol Attacks:
4. Unintentional DoS Attack

Levels of DoS Attacks
1. Flood attack
2. Ping of death attack 3. SYN attack
4. Teardrop attack
5. Smurf attack
6. Nuke
Tools Used to Launch DoS Attack
1. Jolt 2
2. Nemesy
3. Targa
4. Crazy Pinger 5. Sometrouble
Tools used to launch DDoS attack
1. Trinoo
2. Tribe Flood Network (TFN) 3. Stacheldraht
4. Shaft
5. MStream

15. Write short notes on SQL Injection and what are the different counter measures to prevent an attack?
SQL Injection
*Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS).
*SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.
*SQL injection attacks are also known as SQL insertion attacks.
*Attackers target the SQL servers - common database servers used by many organizations to store confidential data
*The prime objective behind SQL injection attack is to obtain the information while accessing a database table that may contain personal information such as credit card numbers, social security numbers or passwords.
*During an SQL injection attack, Malicious Code is inserted into a web form

16. What are the steps involved for SQL Injection attack?
Following are some steps for SQL injection attack:
*The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc.

*To check the source code of any website, right click on the webpage and click on "view source" ,source code is displayed in the notepad.
*The attacker inputs a single quote under the text box provided on the webpage to accept the username and password.
*The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

17. What is blind SQL Injection attack? Can it be prevented?
Blind SQL Injection
*Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.
The page with the vulnerability may not be the one that displays data. Using SQL injections, attackers can:
*Obtain some basic information if the purpose of the attack is reconnaissance. *May gain access to the database by obtaining username and their password. *Add new data to the database.
*Modify data currently in the database.

18. Write a short notes on buffer overflow attacks
Buffer overflow
*Physical memory storage used to temporarily store data while it is being moved from one place to another.
*Buffer is an area of memory used to temporarily store data while it's being moved from one place to another.
*Cache is a temporary storage area used to store frequently accessed data for rapid access.
*Where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations Jab buffer full hota hai toh uska pointer adj mem locn ko overwrite kar sakta hai aur hacker udhar apna malicious code daal kar excecute karwa sakta hai

Types of Buffer Overflow Attacks
*Stack-based buffer overflows are more common, and leverage stack memory that only exists during the execution time of a function.
*Heap-based attacks are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

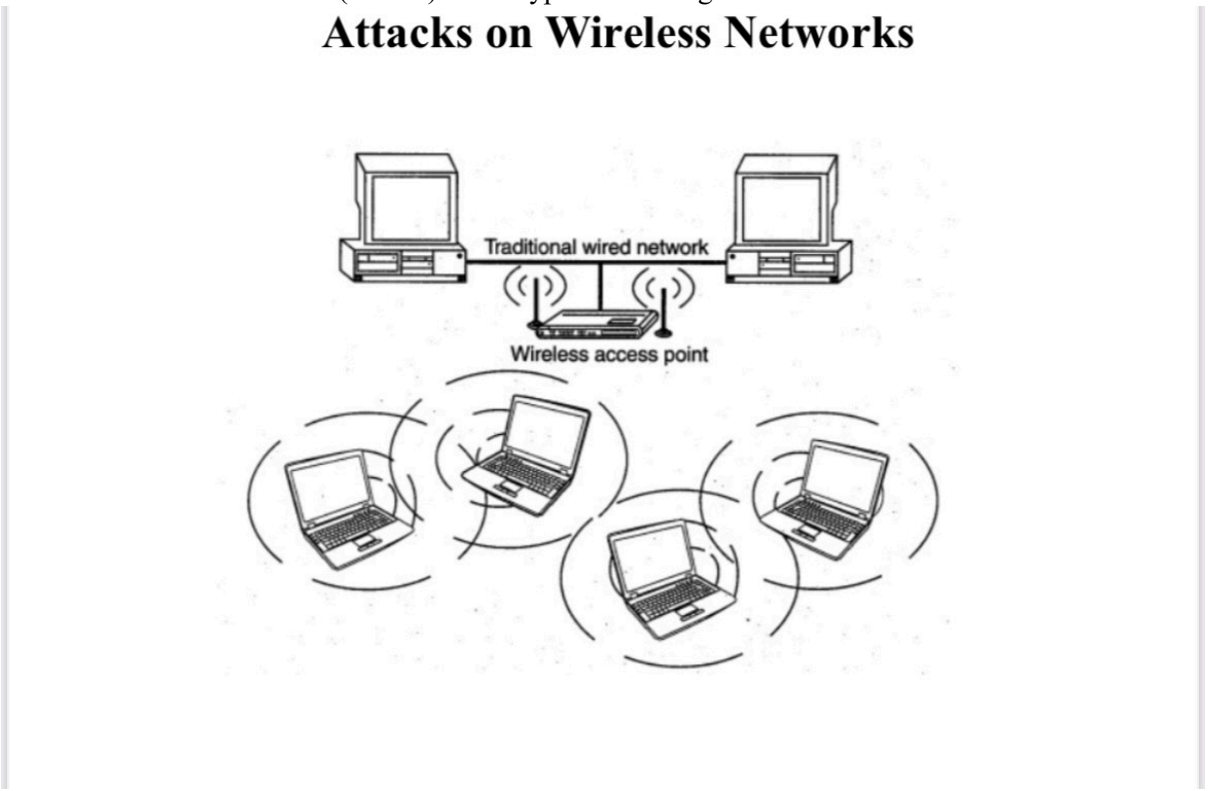
*C and C++ are two languages that are highly susceptible to buffer overflow attacks
*They don't have built-in safeguards against overwriting or accessing data in their memory
*PERL, java, javascript, and C# use built-in safety mechanisms that minimize the likelihood of buffer overflow.

19. Explain in detail about Attacks on Wireless Networks.
Different Types Of "Mobile Workers".
1. Tethered/remote worker:
Generally remains at a single point of work, this includes home workers, tele- cottagers and, in some cases, branch workers.
2. Roaming user:
Works in an environment (E.G., Warehousing, shop floor, etc.) Or in multiple areas (E.G., Meeting rooms).
3. Nomad:
Modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.
4. Road warrior:
The ultimate mobile user

Different Components of Wireless Networks
1. 802.11 networking standards

2. Access points
3. Wi-Fi hotspots
4. Service set identifier (SSID)
5. Wired equivalence privacy (WEP)
6. Wi-Fi protected access (WPA and WPA2) 7. Media access control (MAC)

Traditional Techniques of Attacks on Wireless Networks
1.Sniffing
2. Spoofing:
3. Denial of service (DoS)
4. Man-in-the-middle attack (MITM) 5. Encryption cracking



20. Explain in detail about Phishing

Phishing

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking .

How Phishing Works?
1. Planning
2. Setup
3. Attack
4. Collection
5. Identity theft and fraud

Methods of Phishing
1. Dragnet
2. Rod-and-reel 3. Lobsterpot 4. Gillnet

Phishing – Techniques
1. URL (weblink) manipulation 2. Filter evasion
3. Website forgery

4. Flash Phishing
5. Social Phishing 6. Phone Phishing

How to avoid being victim of Phishing attack
1. Keep antivirus up to date
2. Do not click on hyperlinks in E-Mails
3. Take advantage of anti-Spam software 4. Verify https (SSL)
5. Use anti-Spyware software.
6. Get educated
7. Firewall
8. Use backup system images 9. Secure the hosts file

21. Explain in detail about Identity Theft.
Identity Theft (ID Theft)
This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get get other benefits.
ID theft is a punishable offense under the Indian IT Act (Section 66C and 66D)
Prime Frauds
1. Credit card fraud (26%) 2. Bank fraud (17%)
3. Employment fraud (12%) 4. Government fraud (9%) 5. Loan fraud (5%)

Types Of Identity Theft
Financial Identity Theft Criminal Identity Theft Identity Cloning Business Identity Theft Medical Identity Theft Synthetic Identity Theft Child Identity Theft.

Techniques of ID Theft
1. Human-based methods:
Direct access to information Theft of a purse or wallet: Mail theft and rerouting: Shoulder surfing
False or disguised ATMs ("skimming")
Dishonest or mistreated employees
2. Computer-based technique
Backup theft
Hacking, unauthorized access to systems and database theft: Redirectors

How to prevent being victim of identity theft
1. Monitor your credit closely
2. Keep records of your financial data and transactions
3. Install security software
4. Use an updated Web browser
5. Store sensitive data securely
6. Be wary of E-Mail attachments and links in both E-Mail and instant messages
7. Stay alert to the latest scams