CNS Assignment No.4

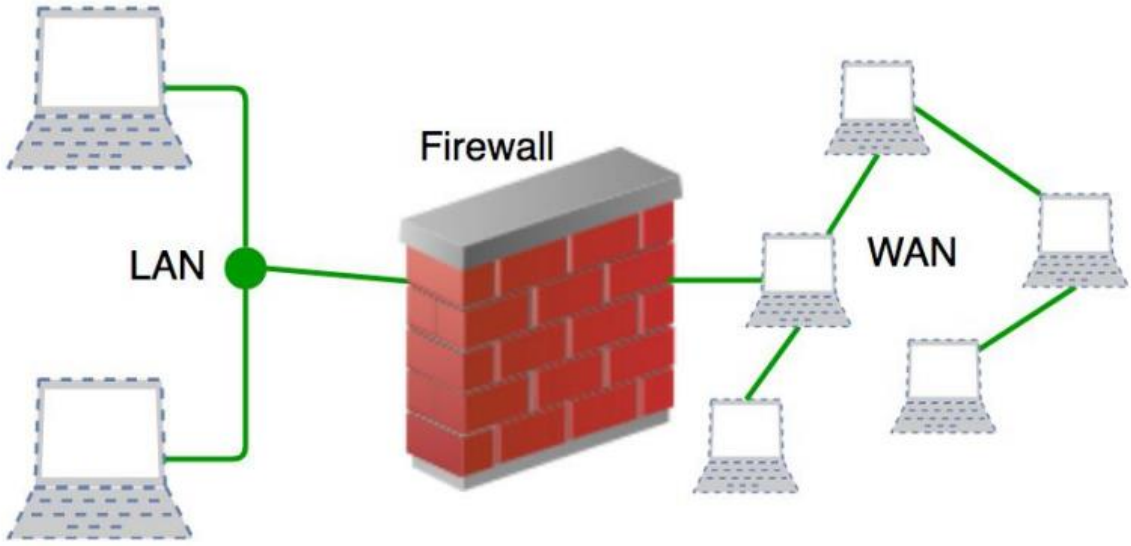
Q1. Describe the term Firewall with neat diagram.

Ans: A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic

Reject : block the traffic but reply with an "unreachable error"

Drop : block the traffic with no reply A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



Q2. Explain the different types of firewalls.

Ans:

A.Software Firewalls:-

A software firewall is installed on the host device. Accordingly, this type of firewall is also known as a Host Firewall.

B. Hardware Firewall:-

As the name suggests, hardware firewalls are security devices that represent a separate piece of hardware placed between an internal and external network.

C. Packet Filtering Firewall:-

When it comes to types of firewalls based on their method of operation, the most basic type is the packet-filtering firewall.

D. Circuit Level Firewall:-

Circuit-level gateways are a type of firewall that work at the session layer of the OSI model, observing TCP (Transmission Control Protocol) connections and sessions.

E. Stateful Inspection Firewall:-

A combination of the two firewalls above, the stateful inspection firewalls offer a higher level of protection for your business. The problem with these is that they take up more resources, which can slow down the legitimate packet transfer.

F. Proxy Firewalls (Application-Level Gateways / Cloud Firewall):-

If you want firewalls that operate at the application layer to filter traffic, proxy firewalls do the job. These are cloud-based most of the time, and they establish traffic connections and examine data packets coming through. The difference between these and the stateful inspection firewalls is that the proxy firewalls can also do a more in-depth inspection to check the packet contents.

Q3. Define viruses and malicious code in details.

Ans:

Code Type	Characteristics
Virus	Attaches itself to program and propagates copies of itself to other programs
Trojan horse	Contains unexpected, additional functionality
Logic bomb	Triggers action when condition occurs
Time bomb	Triggers action when specified time occurs
Trapdoor	Allows unauthorized access to functionality
Worm	Propagates copies of itself through a network
Rabbit	Replicates itself without limit to exhaust resource

Q4. Why we need to protect the computer resources?

Ans: Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system.

We can take protection as a helper to multi programming operating system, so that many users might safely share a common logical name space such as directory or files

Protection and security require that computer resources such as CPU, softwares, memory etc. are protected.

Need of Protection:-

- To prevent the access of unauthorized users.
- To ensure that each active programs or processes in the system uses resources only as the stated policy.
- To improve reliability by detecting errors.

Computer Resources has threats from the following:-

- Viruses.
- Trojan Horse.
- Trap door.
- Worm.
- Denial of Service.

Q5. How we can protect the computer resources?

Ans: The different methods that may provide protect and security for different computer systems are –

A.Authentication:-

This deals with identifying each user in the system and making sure they are who they claim to be. The operating system makes sure that all the users are authenticated before they access the system. The different ways to make sure that the users are authentic are:

- **Username/Password:-**

Each user has a distinct username and password combination and they need to enter it correctly before they can access the system.

- **User key/User Card:-**
  The users need to punch a card into the card slot or use they individual key on a keypad to access the system.
- **User attribute identification:-**
  Different user attribute identifications that can be used are fingerprint, eye retina etc. These are unique for each user and are compared with the existing samples in the database. The user can only access the system if there is a match.

B.One Time Password:-

These passwords provide a lot of security for authentication purposes. A one time password can be generated exclusively for a login every time a user wants to enter the system. It cannot be used more than once. The various ways a one time password can be implemented are –

- **Random Numbers:-**

  The system can ask for numbers that correspond to alphabets that are pre arranged. This combination can be changed each time a login is required.

- **Secret Key:-**
  A hardware device can create a secret key related to the user id for login. This key can change each time.

Q6. Explain the firewall configuration process in details.

Ans:

Checking Firewall Settings on a PC:

1. Open your Start menu. Windows' default firewall program is located in the "System and Security" folder of the Control Panel app, but you can easily access your firewall's settings.
2. Type "firewall" into the search bar. Doing so will automatically search your computer for applications matching your typing.
3. Click the "Windows Firewall" option.

Your computer's firewall is largely responsible for blocking incoming connections that could potentially harm your computer. You can view and alter your firewall settings on any computer, but keep in mind that the firewall application is best applied to PCs; Mac users usually need not enable or use the built-in firewall program.

Q7. What are the different types of malicious code/threats occurs in a computer system?

Ans: Targeted malicious code is written for a particular system. To do so the attacker or the code writer studies the system carefully identifying its weaknesses. The different types are:

- **Brain:**
  The Brain virus placed itself in the boot sector and other places on the system. It then screened all disk access so as to avoid detection and to maintain its infection. Each time the disk was read, Brain would check the boot sector to see if it was infected. If not, it would reinstall itself in the boot sector and elsewhere. This made it difficult to completely remove the virus.

- **Morris Worm:**
  The Morris worm obtains a remote access to machines on the network by guessing the user account passwords. If that failed, it tried to exploit a buffer overflow and also tried to exploit a trapdoor in send-mail.
- **Code Red:**
  To gain access to a system, the Code Red worm exploited a buffer overflow in Microsoft IIS server software.
- **SQL Slammer:**

  The Slammer infects sites by randomly generating IP addresses. Slammer spreads too fast and effectively burns out the available bandwidth on the Internet.

- **Time Bomb:**
  This is a code that it will take effect at a particular time or date. The virus is stored in the memory till it is time to burst. Y2K is a good example of time bomb.
- **Logic Bomb:**
  It is a malicious code initiated when a specific condition occurs. Logic can be with respect to some event. The logic can be a condition or a count which remains in the memory for the condition to occur and affect the system.

Q8. What are the different types of protection & security methods used in computer system?

Ans: The different methods that may provide protect and security for different computer systems are –

A.Authentication:-

This deals with identifying each user in the system and making sure they are who they claim to be. The operating system makes sure that all the users are authenticated before they access the system. The different ways to make sure that the users are authentic are:

- **Username/Password:-**

Each user has a distinct username and password combination and they need to enter it correctly before they can access the system.

- **User key/User Card:-**
  The users need to punch a card into the card slot or use they individual key on a keypad to access the system.
- **User attribute identification:-**
  Different user attribute identifications that can be used are fingerprint, eye retina etc. These are unique for each user and are compared with the existing samples in the database. The user can only access the system if there is a match.

B.One Time Password:-

These passwords provide a lot of security for authentication purposes. A one time password can be generated exclusively for a login every time a user wants to enter the system. It cannot be used more than once. The various ways a one time password can be implemented are –

- **Random Numbers:-**

  The system can ask for numbers that correspond to alphabets that are pre arranged. This combination can be changed each time a login is required.

- **Secret Key:-**
  A hardware device can create a secret key related to the user id for login. This key can change each time.

Q9. List out Secure Computing Tips.

Ans:

- **You are a target to hackers:**
  Don't ever say, "It won't happen to me." We are all at risk and the stakes are high - both for your personal and financial well-being and for the university's standing and reputation
- **Keep software up-to-date:**
  Installing software updates for your operating system and programs is critical. Always install the latest security updates for your devices
- **Avoid Phishing scams – beware of suspicious emails and phone calls:**
  Phishing scams are a constant threat - using various social engineering, cyber-criminals will attempt to trick you into taking out personal information such as your login ID and password, banking or credit card information.
- **Practice good password management:**
  We all have too many passwords to manage - and it's easy to take short-cuts, like reusing the same password. A password manager can help you to maintain strong unique passwords for all of your accounts. These programs can generate strong passwords for you, enter credentials automatically, and remind you to update your passwords periodically.
- **Be careful what you click:**
  Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically install (often silently) and compromise your computer.
- **Never leave devices unattended:**
  The physical security of your devices is just as important as their technical security. If you need to leave your laptop, phone, or tablet for any length of time - lock it up so no one else can use it. For desktop computers, lock your screen or shut-down the system when not in use

- **Safeguard Protected Data:**
  Be aware of Protected Data that you come into contact with and its associated restrictions. Review the UCB Data Classification Standard to understand data protection level requirements. Always use encryption when storing or transmitting sensitive data.

- **Use mobile devices safely:**
  Considering how much we rely on our mobile devices and how susceptible they are to attack, you'll want to make sure you are protected:
  Lock your device with a PIN or password - and never leave it unprotected in public.
  Only install apps from trusted sources (Apple AppStore, Google Play).
  Keep the device's operating system up-to-date.
  Don't click on links or attachments from unsolicited emails or texts
- **Install Antivirus/Anti-malware protection:**
  Only install these programs from a known and trusted source. Keep virus definitions, engines and software up-to-date to ensure your programs remains effective.
- **Backup your data:**
  If you are a victim of a security incident, the only guaranteed way to repair your computer is to erase and re-install the system. Keeping backup up of data will help you in getting all the data as it was.

Q10. What are the different methods of control provide to security of data.

Ans: The following are the main control measures are used to provide security of data in databases:

1. **Authentication:**
   Authentication is the process of confirmation that whether the user log in only according to the rights provided to him to perform the activities of data base. A particular user can login only up to his privilege but he can't access the other sensitive data. By using these authentication tools for biometrics such as retina and figure prints can prevent the data base from unauthorized/malicious users.
2. **Access Control:**
   The security mechanism of DBMS must include some provisions for restricting access to the data base by unauthorized users. Access control is done by creating user accounts and to control login process by the DBMS. So, that database access of sensitive data is possible only to those people (database users) who are allowed to access such data and to restrict access to unauthorized persons. The database system must also keep the track of all operations performed by certain user throughout the entire login time.
3. **Inference Control:**
   This method is known as the countermeasures to statistical database security problem. It is used to prevent the user from completing any inference channel. This method protect sensitive information from indirect disclosure. Inferences are of two types, identity disclosure or attribute disclosure.
4. **Flow Control:**

This prevents information from flowing in a way that it reaches unauthorized users. Channels are the pathways for information to flow implicitly in ways that violate the privacy policy of a company are called convert channels.

5. **Encryption:**
   This method is mainly used to protect sensitive data (such as credit card numbers, OTP numbers) and other sensitive numbers. The data is encoded using some encoding algorithms. An unauthorized user who tries to access this encoded data will face difficulty in decoding it, but authorized users are given decoding keys to decode data.