# Assignment # 2

## CSCI 22062- Introduction to Cyber Security
## Faculty of Computing & Technology
## University of Kelaniya.

K.B. Kavinda

**CS/2018/021**

1. **What are the differences between Key Distribution Center (KDC) and Certification Authority? What are the strengths and weaknesses of the two approaches?**

    Key Distribution center is a place that provide a symmetric key to users. Each key is symmetric encryption which is unique ticket type key to share sensitive or private data each other. the main role of KDC is authenticate users and distribute tickets of information which are stored in database. When client receive the ticket and submit to the appropriate server, it will verify it and give permission to access. KDC use Kerberos as its security background. In general uses, KDC use in small networks not for big one.

    When the process of creating public key cryptography, Certification Authority generate digital certificate. These keys are used in SSl protocols to activate secure session on web pages. When a user log into any site that implement the HTTP secure protocol. then we can maintain a secure session between browser and the web server.

    By using Multiple domains single KDC/CA could find solutions for several problem. When we use multiple KDC, it can share pairwise keys also CA can perform cross-certifications of CAs.

**2. Describe the step-by-step authentication process used in Kerberos.**

Kerberos is the present authorization technology which used in Microsoft Windows. It was introduced with windows2000.

There are mainly several steps to authenticate in Kerberos

1) The client requests an authentication ticket from the KDC
2) KDC verifies credentials and send ack an encrypted ticket and session key
3) The ticket is encrypted through the Ticket Granting Service
4) The client stores ticket and when it expires the local session manager will request another ticket.
5) The client sends the current ticket to the Granting service with service principal name
6) KDC verify the ticket of the user and give access to the service
7) TGS send a valid session key
8) Client forwards the session key to the service

**3. Discuss the concepts of layered security and Diversity of Defense used in security.**

Layered security approach is a security strategy for multiple components to protect operations on multiple levels or layers. firewall is only one component of a layered security strategy and layered security is only one component of diversity of defense.

DD is designed to protect physical, technical and administrative aspects of the network. There are several strategies we can find,

Monitoring response
disaster recovery
forensic analysis

DD provides ensuring rapid notification, threat delay and response when attacks and disasters are going to happen. So it will keep in touch with unexpected threats and give flexible policies that responds with new conditions.

**4. Compare and contrast Authentication and Access Control.**

| Authentication | Access Control |
|---|---|
| ❖ The system verify the identity of the user who have to access to enter the system.<br>❖ The user or computer has to prove its identity<br>❖ Implementation is done through the user name & password, fingerprint, etc<br>❖ Usually done before access control | ❖ The system will check if the client has permission to use of access to the resource file.<br>❖ Give permission to create, read, edit files.<br>❖ usually done after successful authentication |

**5. Discuss the steps of hacking in details.**

1) Find the target

A hacker decided to hack any system, he or she must gather information as much as the can. we can call it as reconnaissance. Hackers find valuable data like password, personal details. Then hacker collect details about the security system, WE called it as footprint.

2) Locate the target's assets (Scanning)

Now hacker can identify the quicker way to access to the network. There are mainly three methods in scanning,

pre-attack - The hacker scans the network
port scanning/sniffing – use data gathering equipment
information extraction – hacker collect information about port, OS

3) Gain access

   The hacker enter to the system, network etc and control them

4) Maintain access

   The hackers launch additional attacks like Trojans

5) Cover Tracks

   Finally, the hacker delete all the cache and cookies, details about open ports. Because it is essential to block the track.

6. **Describe different types of vulnerabilities related to information technology. Discuss the importance of identifying vulnerabilities of your own organization.**

   Vulnerability is a most common part in our day to day projects. Although the new technology are introduced there are so many vulnerabilities can happen. we can divide those in several types,

   Hardware :- As the weakness of the system hardware physically or remotely attack can be happened

   - Old version system not supported with new drives
   - Unprotected storage

   Software :- When the errors happens in development and configuration process, security policies can be violated.

   - Buffer overflow
   - Lack of input validation
   - Unencrypted data

Network :- The weakness which are happened in network

- Unprotected communication

  The main reason for communication vulnerabilities is lack of authentication, by that fake details of virus can attack to the system.
- Malware or malicious software
- Social engineering attacks

Procedural :- as the result of the weakness of organization operational methods

Password procedure(password should follow standard policies)

Training procedure

Knowingly or unknowingly vulnerabilities can be happened. We can strong our security environment by using better KDC server or CA server, because security is most important part in an organization. Also if we maintain a better knowledge with upcoming technologies it will reduce the issues in physical and software vulnerabilities.

**7. Discuss the use of different types Firewalls and IDS for protecting a IT infrastructure of an organization.**

Firewall is a security platform that can protect internal network from the outside malicious traffic. It is like a filter. The firewall works with set of rules for this security process. Packet filtering firewall, Circuit level Gateways, Application-level Gateways are main firewalls that can see.

Packet Filtering :- This is very basic type firewall. The base of this firewall is network layer, so it is connected to the internet via router. Source IP, destination IP, the protocol etc are checked.

Packet filtering Firewalls are fast, easy to use but the security background is basic.

Circuit-level Gateway:- It provides User datagram protocol(UDP) and Transmission Control Protocol(TCP) connection security

Application-level Gateway :- The process of the application level gateway, implementation is done via proxy devices. so we called it as proxy firewall. the security is better than the packet filters and also easy to log and audit all traffics. The main disadvantage is we need more performance for this proxy firewall.

IDS

IDS can be a device or software application that monitor network traffic for malicious activities and generate alerts. it detect real time traffic and looks for traffic patterns.

we can divide IDS to several types, among that host-based and network-based are the types of deployment.

Host-based :- HIDS is a host or devices on the network. It monitors income and outgoing malicious activities and give alert to the administrator. Basically it monitor the process of the computer.

Network-based :- It designed to monitor an protected network. NIDS has visibility into all traffic through the network but the performance of internal visibility is low.

And also misuse and anomaly are detection method of IDS

Misuse Detection :- It detects the attacks which have a specific pattern, also detect malicious sequence which are already known. it means this approach can't detect new attacks. so we called this IDS as Signature-based IDS

Anomaly Detection :- This IDS has a static based. It designed to detect malware attacks. the development is build through a machine learning platform.

Basically, firewall and ids are security network. But the process is different. Firewall designed to stop malicious activities before it happens and IDS designed to give alert to the administrator if some malicious activity happen.