Q1] Explain the evolution of information Security

Ans In the early days of networking individual computers were connected together only in academic and governme-nt environments. Thus at the time the networking technologies that were developed were specific to academic security model was "wide open" and the government security model was "closed" and "locked" There wasn't much in between The government was mainly concerned with blocking access to computers, restricting internal access to confidential data and preventing interception of data This method of protecting assets, provide a hard-to-penetrate perimeter as depicted In the academic world the goal was to share information openly so security controls were limited to accounting functions in order to charge money for the use of computer time. Note that these two models are diametrically opposite the governments model blocks everything There is plenty of room in between these two extremes In the field of computers security the practices established by the academic and government institutions persisted until the early 1990s and some of the Practical are still around today Those practices that have endured continue to have their place in a comprehensive security strategy but they are no longer sufficient to meet the

needs of the modern computer network As the use of information technologies evolved the original all or nothing approaches to security no longer met the needs of information consumers. So the practice of network security evolved The concepts of intranets and extranets ~~and~~ were developed to accommodate internal and external consumers, respectively with secured boundaries that resembled miniature versions of a firewall perimeter Virtual private network (VPNs) were developed to provide a secure channel (or tunnel) from one network to another. These approaches continued through the end of the 1990s to the early part of the 2000s after which the first edition was published.

Q2] What are the different sources and targets of threat

Ans There are plenty of other books available that cover everything you ever wanted to know about hacking and many of them are really good This book is about defence-protecting against attacks Nevertheless as a security practitioner you need to understand how attacks work so that you can select the best countermeasures for defense. This chapter provides and some common countermeasures to protect against those attacks The goal is to equip you with the knowledge principles and perspective needed to implement the right countermeasures the environment

Security controls can be logically grouped into several categories:

- Preventative: Block security threats before they can exploit a vulnerability
- Detective: Discover and provide notifications of attacks or misuse when they happen
- Deterrent: Discourage outsider attacks and insider policy violations
- Corrective: Restore the integrity of data or another asset
- Recovery: Restore the availability of a service

Compensative: In a layered security strategy provide protection even when another control fails.

Each category of security may have a variety of implementations to protect against different threat vectors:

- Physical: Controls that are physically present in the "real world".
- Administrative: Controls defined and enforced by management
- Logical / technical: Technology controls performed by machines.
- Operational: Controls that are performed in person by people.
- Virtual: Controls that are triggered dynamically when certain circumstances arise.

Q3.] Explain the concept of 'CIA' triad in breif.

Ans Every security book written in the last several years mentions the CIA triad- confidentially, integrity and availability. This venerable well established conceptual model though very data centric is often useful in helping people think about security in terms of the most important aspects of information protection. The CIA concept is not perfect. CIA focuses on three aspects of information protection that inded are important, but it is not an all-inclusive model.

- Confidentiality:
Confidentiality refers to the restriction of access to data only to those who are authorized to use it. Generally speaking this means a single set of data is accessible to one or more authorized people or systems, and nobody else can see it. Confidentiality is distinguishable from privacy in the sense that confidential implies access to one set of data by many sources while private usually means the data is accessible only to a single source.

- Integrity:
Integrity which is particularly relevant to data refers to the assurance that the data has not

been altered in an unauthorized way Integrity controls are meant to ensure that a set of data can't be modified (or deleted entirely) by an unauthorized party But part of the goal of integrity controls is to block the ability of unauthorized people to make change to data and another part is to provide a means of restoring data back to a known good state.

- Availability

Unlike confidentiality and integrity, which make the most sense in the context of the data contained within computer systems availability refers to the uptime of computer-based services - the assurance that the service will be available when its needed. Service controls on computers networks and storage. High availability (HA) pairs or clusters of computers redundant network links and RAID disks are examples of mechanisms of protect availability.

Q4] Explain the role based authorization in brief

Ans Each job within a company has a role to play Each employee requires privileges (the right to do some thing) and permissions (the right to access particular resources and do specified things with them) if they are do their job Early designers of computer system recognized that the needs of possible users of system would vary and that not all users should be given the right to administer the system.

Two early roles for computing systems were those of users and administrator. Early system defined roles for these types of users to play and granted then access based on their membership in one of these two groups. Administrator (superusers root, admins and like) ~~ad~~ were granted special previlage and allowed access to a larger assay of computer resources than were ordinary users. Administrator for example could add users, assign passwords, access system files and programs & reboot the machine. Ordinary users could log in and perhaps read data, modify it and execute programs. This grouping was later extended to include the role of auditor. As system grew the role of users were made more granular Users might be quantified by

their security clearance for example and allowed access to specified data or allowed to run certain applications. Other distinctions might be made based on the user's role in a database or other applications system. Commonly roles are assigned by departments such as Finance, Human Resources, Information technology and sales.
In the simplest examples of these role-based systems users are added to group that have specific rights and privileges. Other role-based systems are more complex systems of access control, including some that can only be implemented if the operating systems is designed to manage them
The Unix-role based access control (RBAC) facility can be used to delegate administrative privileges to ordinary users. It works by defining role accounts or accounts that can be used to perform certain administrative tasks. Role accounts are not accessible to normal logon's they can only be accessed with the 'su' command.

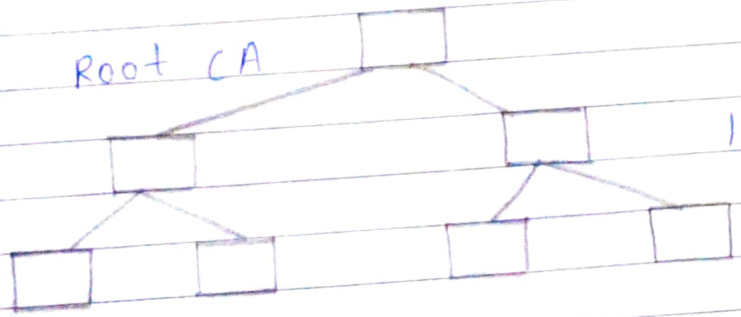
Q5] What is the CA hierarchy of public key infrastructure in brief?

Ans Public key Infrastructure (PKI) has become one of the most prevalent forms of encryption in modern electronic transactions. An associated key pair is bound to a security principal (user or computer) by a certificate. The certificate also makes the security principal's public key available while the related private key is kept hidden. A certificate authority (CA) issues, catalogs, renews and revokes certificates under the management of a policy and administrative control. There is no need either to purchase third-party products to do so, or to purchase individual certificates from public CAs. Newer versions of window server have continued to provide CA services and to add functionality. For example, window server 2003 enterprise CAs offer version 2 certificate templates and window server 2008 enterprise CAs offer version 3 certificate templates to allow for further control and customization.

Multiple CAs can be arranged in a hierarchy for security, redundancy and geographical and functional diversity. CAs can issue various type of template. A user or computer must have a

template designed and approved for a specific use in order to participate in a have a template designed and approved for a specific use in order to participate in a specific function such as encryption files or using a smart card or enrolling other users.

In a hierarchy one root CA provides CA certificates for another level of CAs while there are many hierarchical designs that can be arranged. the classic, best practice design is displayed in the figure. In this design the root CA is kept offline and produces CA certificates only for the next, intermediary level of CAs. These CAs are integrated with AD and kept online. They issue certificates for a third level the issuing CAs that actually issues certificates for end use such as EFS or smart cards, ~~ba~~ Issuing CAs do not issue (a certificate.



Q6] What are the best practices available to design a robust architecture that is resistant to attack

Ans The following practies provide the best available mitigation:

Zoning

Port-based zoning improves security through control of the connections between hosts and the storage array. This method of zoning provides increased protection against a WWN spoof attack. With port zoning even if a host system is introduced into the environment with a spoofed WWN, the host would need to also to be in the port defined by the switch in order for its traffic to transmit to the storage array because the zones are configured based on ports. The switch provides the path by way of the zone, from the server's HBA to the array's HBA. without that zone, the spoofed WWN has no path to the array.

Arrays

Arrays have been developed over time to provide LUN masking as a form to protecting LUNs from access by unauthorized servers. The most likely cause of a LN being accessed by an unauthorized system is accidential or intentional misconfiguration by a storage administrator. The best defence

against this is to cause that storage administrator are trustworthy and capable and to control and limit the management of the storage array to a small number of highly trained reliable administrator.

- Servers
In order to fully secure a storage environment you must ensure that the server environment itself is controlled and monitored. Securing the storage infrastructure itself is not enough. Access to any server can significantly expose the server and the storage environment to harmful activity. It is important that servers be configured securely and that the equipment is located in a secure facility with access control and monitoring.

- Offsite Data storage.
Storing data offsite (securely) is a critical aspect of any organization's business continuity process. Many vendors will pick up backup tapes and moves them to a secured ability. Regular audits to these facilites should be done to ensure accountability for all data sent offsite. To protect the data, it should be encrypted whether on disk or tape. Any form of online data backup should be with end to end encryption.

Q7.] Explain the layers of CISCO hierarchical inter network model

Ans The CISCO hierarchical Internetworking model uses three main layers commonly referred to as the core, distribution and access layers.

Core layer:
Forms the network backbone and is focused on moving data as fast as possible between distribution layers. Because performance is the core layer's primary focus. it should not be used to perform CPU intensive operations such as filtering, compressing, encrypting or translating network addresses for traffic

Distribution layer
Sits between the core and the access layer This layer is used to aggregate access-layer traffic for transmission into and out of the core.

Access layer
Composed of the user networking connections.

Filtering, compressing encrypting and address-translating operations should be performed at the access and distribution layers.
The CISCO model is highly scable. As the

network grows, additional distributions and access layers can be added seamlessly. As the need for faster connections and more bandwidth arises, the core and distribution equipment can be upgraded as required. This model also assists corporations in achieving higher levels of availability by allowing for the implementation of redundant hardware at the distribution and core layers. And because the network is highly segmented a single network failure at the access or distribution layers does not effect the entire network.

Although the Cisco three tire model is perhaps the most commonly known and referenced model for designing LAN environments, it has its limitations and is rapidly being supplanted by newer models aimed at addressing the specific needs of highly virtualized data centers by the specific needs at different industry verticals and the specific needs of cloud computing and multitenancy environments.

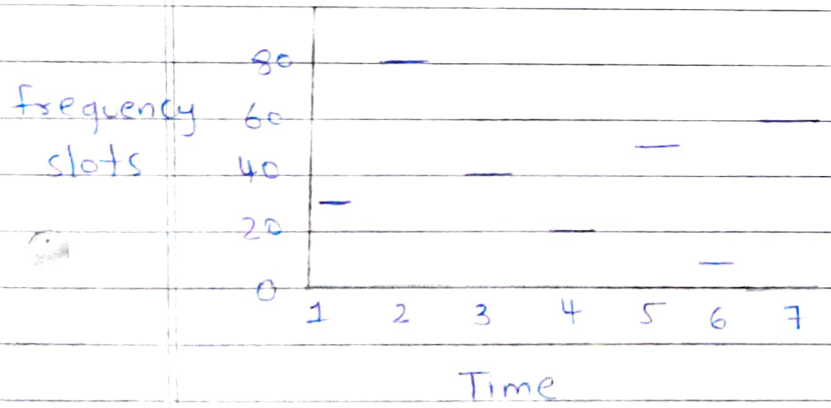
Qs] Explain different types of routing protocol

Ans There are two main types of layer three routing protocols distance-vector protocols and link state protocols The main difference between the two types is in the way they calculate the most efficient path to the ultimate destination network. Distance-vector protocols are more simplistic are better suited for smaller network and requires less CPU power on the devices that run them. Distance vector protocols maintain tables of distance to other networks Distance is measured in terms of hops, with each additional router than a packet must pass through being considered a hop. The most popular distance vector protocol is the Routing Information Protocol (RIP).
Link state protocols were developed to address the specific needs of larger networks. Link state protocols use several different metrices to determine the best route to another network and the maintain maps of the entire network, that enable them to determine alternative and parallel routing paths to remote networks Open Shortest path First (OSPF) and Intermediate System to system (IS-IS) are examples of link-state protocol Link state protocol metric calculation and maintain databases of the entire network

topology, and require significantly more CPU and memory capability than distance-vector protocols As router hardware has evolved and more functions have been handled in silicon, such as in Cisco's Content Addressable Memory (CAM) and Ternary content Addressable Memory (TCAM) a type of memory used by Cisco devices even low end routers can generally handle link state routing. For networks to function properly all routers in a given network must maintain the same view or topology of the network and the process by which routers come to agree upon the network topology is called convergence. Distance vector and link state protocols use different mechanisms to converge. The ability of a routing protocol to detect and respond to change in network topologies is a significant advantage over the use of static routes.

Q9] Explain frequency hoping spread spectrum with neat diagram

Ans In FHSS a pseudorandom sequence of frequency changes (hops) is followed by all hosts participating in a wireless network.
The carries remain at given frequency for a dwell time period and then hops to another frequency (spending a hop time to do it); the sequence is sequence is repeated when the list of frequencies to hop through is exhausted. FHSS was the first spread implementation technology proposed.



It is used by legacy 1-2 Mbps 802.11 FHSS network and most importantly, 802.15 networks (Bluetooth) Bluetooth hops 1600 times per second (≈625 μs dwell time) and must hop through at least 75 MHz of bandwidth in the middle ISM band. As such bluetooth is very resistant to radio

interference unless the interfering signal covers the whole middle ISM band. At the same time, bluetooth devices introduce wideband interference capable of disrupting 802.11, 802.11b, and 80.211g LANs. Thus a bluetooth enabled phone. PDA or laptop can be efficient wideband DOS / jamming tool against other middle ISM band wireless network.

As to interference issues arising from using multiple ~~three~~ Bluetooth networks in the same area, it is theoretically possible to keep 26 Bluetooth networks in the same area owing to the different frequency hopping sequences on these networks. In practice however exceeding 15 networks per area is not recommended, but the time when widespread bluetooth use will create such a density of network is coming. and is closer than it seems - college now plan for 7 devices per use ~~of~~ for campus-provided wireless networks. You can imagine that in a dorm room with 4 to 6 tenants in close proximity, the number of bluetooth network could easily exceed 15 networks.