NAT:

The Network Address Translation allows private IP address to be used in the public internet and this is done by using the alias public IP addresses replacing the private IP address when the packets are sent to the public internet. The NAT router then reverse the process when the packets are sent from Public internet to the internal network. The NAT are required because the private IP addresses cannot be used beyond the internal network and only public IP can route in the internet. The Port Address Translation is another variation of NAT that uses single IP address for all the Private IPs, but a different TCP port number.

NAT also provides security:

The NAT router keep track of all the packets sent and received, so it discards the unsolicited packets and prevents from reaching to the internal network.

NAT masked the IP addresses of the internal devices, and therefore if an attacker sniffs the packets on the internet cannot determine the actual IPs of the devices. The attacker only gets the Public IP that is being used for translation.

NAC

Network Access Control evaluates the current states of the devices or system against the specified standard that is created for a network like having updated antivirus software or firewall software properly configured. If any devices didn’t meet the specified set of standard then they are allowed to connect to a quarantine network where the specified deficiencies are corrected. After the correction, devices are allowed to connect to the normal network.

NAC process:

* Client performs self-assessment using a System Health Agent (SHA) to determine the current security state.
* The assessment know as a Statement of Health (SoH), is sent to the server called Health Registration Authority (HRA). The HRA enforces the security polices and evaluate the SoH of the client.
* The approved client are given the Heath Certificate, which can be presented to the network server to verify that the client’s security condition has been approved.
* If the client is not approved, it is then allowed to connect to the quarantine network where the deficiencies are corrected, and after that devices are allowed to connect to the production network.

The NAC uses the DHCP method and ARP poisoning method to allow the client to connect to the quarantine and production network.

VLAN

The virtual Local Area Network is a technique that allows the logical grouping of the devices/users and are independent of the location. The devices/users can be physically attached to different switches yet can be in the same VLAN. When the traffic is broadcasted/unicasted only the member of the same VLAN can received it unless a router is used for intra-VLAN routing. The routing between the same VLAN can be handled by the switch itself, while a router is required for intra-VLAN routing. VLAN is a secured way of grouping the devices/users.

**Firewalls:**

The firewall inspects the packets and either accept or deny the entry. The modern firewall do more than just inspecting the packet header for IP numbers and port numbers. Firewall filtered the packets in one of two ways: Stateless packet filtering in which, the firewall just inspect the packets based on the rules setup by the administrator and permits or denies it. In the second method, stateful packet filtering, the firewall keeps the record of a state of a connection between the internal and external devices and makes the decision based on the connection state as well as the conditions.

Firewall perform different actions on the packet received like allow the packet to pass, drop the packet without sending any response to the sender, reject the packet and send message to the sender or ask what action to take.

The Rule-Based firewall used the firewall rules, set of instructions to control actions. The rules contains:

* Source address: IP address, Mac address or hostname of the sender
* Destination address:
* Source Port: source TCP/IP port numbers
* Destination Port:
* Protocol: Protocol being used like TCP, UDP, IP, ICMP
* Direction: direction of traffic, IN or Out
* Action: what the firewall do when conditions are met. Allow, Drop, Reject or Ask.

Policies and Procedures:

Security policies is a written document that states how an organization plans to protect the organization information technology assets. The policy outlines the protections that should be enacted to ensure the organizations assets face minima risk.

Functions of security policy:

* It create the security awareness within the employee and develop an organizational culture
* It help to ensure that employee behavior is directed and monitored in compliance with security requirments
* It details specific risk and how to address them.

A guideline is a collection of suggestions that should be implemented. A policy is a document that outlines a specific requirements or rules that must be met.

Characteristics of policies:

* Defines appropriate behavior for users
* Identifies what tools and procedures are needed
* May be helpful if it is necessary to prosecute a violator
* Communicates a consensus of judgement.

The security Policy Cycle: Three phase cycle in developing and maintaining a security policy.

* Vulnerability assessment (asset identification, threat evaluation, vulnerability appraisal, risk assessment, risk mitigation)
* The second phase is to use the information from the risk management study to create the policy.
* The final phase is to review the policy for compliance. Because new assets are continually being added and new threats appear against the assets, compliance, monitoring and evaluation must be conducted regularly.

Policy must do:

* Be complement and enforceable
* Be concise and easy to understand
* Balance protection with productivity

Security policy should:

* State reasons why the policy is necessary
* Describe what is covered by the policy
* Outline how violations will be handled

Guidelines for developing the policy:

* Notify users in advance and explain why policy is needed
* Provide the sample of people affected by the policy
* Prior to deployment, give all users at least a week to review the policy

Types of security Policies:

* Email policy
* Email retention policy
* Router security policy
* VPN security policy
* Wireless communication policy
* Antivirus policy
* Acceptable Use Policy (ACP)
* Privacy Policy
* Data Policies
* Security-related HR Policy
* Ethics Policy
* Password Management and Complexity Policy

Awareness and Training involves instructions regarding compliance, secure user practices, and an awareness of threats.

Compliance: Users should be made aware of the organiztions established security strategies as well as the reasons why it is necessary to adhere to it. Users should be informed of:

* Security policy training and procedures
* Personally Identifiable Information (PII)
* Information Classification
* Data labelling, handling, and disposal
* Compliance with laws, best practices and standards

Social Networking

Additional risks:

* Personal data can be used maliciously
* Users may be too trusting
* Accepting friend may have unforeseen consequences
* Social networking security is lax or confusing

Defense Mechanisms:

* What information is posted on these sites
* Who can view their information
* Updated with the security settings of the sites as it is frequently updated. Disable options of feature until it is necessary.

Slack Space:

Slack Space: A form of residual data, slack space is the amount of on-disk file space from the end of the logical record information to the end of the physical disk record. Slack space can contain information soft-deleted from the record, information from prior records stored at the same physical location as current records, metadata fragments and other information useful for forensic analysis of computer systems.' From the Kroll Ontrack Glossary.

Slack space is a form of internal fragmentation, i.e. wasted space, on a hard disk. When a file is written to disk it’s stored at the “beginning” of the cluster. A cluster is defined as a collection of logically contiguous sectors and the smallest amount of disk space that can be allocated to hold a file.

Rarely will there be an even match between the space available in a cluster (or collection of clusters for longer files) and the number of bytes in the file. Left over bytes in the cluster are unused, hence the name slack space.

**List and describe two of the seven risk categories.**

The two risk categories are:

Environmental: The risk from the natural forces like tornado, floods, volcano, earthquake and so on. These risks are unavoidable and has a great impact.

Technical: The technical risks are related to the operation of the information technology systems. The events like DoS, DDoS, SQL injection attack, phishing, virus and malware attack are the technical risk.

**List four attributes that should be compiled for new equipment in the change management documentation.**

The four attributes that should be complied for new equipment in the change management documentation are:

IP and Mac address

Equipment name and type

Location

Manufacturer, serial number model and part number

**List two characteristics of a policy.**

The two characteristics of policy are:

Defines appropriate behaviors for users

Identifies the required tools and procedure

**Which roles should be represented on the security policy development team?**

The roles that should be represented in the policy development team are:

Senior-level administrator

Member of management

Member of the legal staff

Representative from the user community

**List one reason why social networking sites are popular with attackers.**

The networking sites are popular with attackers because attackers can get lots of personal information of the user, can gain trust of the user and these information are useful in social engineering attacks.

**What is a general security tip for using a social networking site?**

The general security tip for using a social networking sites are:

be cautious on what to share or post

be cautious on who can view your information and

be cautious and updated with the security setting, features of the social networking sites

**Identify two opportunities for security education and training.**

The two opportunities for security education and training are:

During orientaion, when a new employee is hired or when an employee is promoted or given new responsibilities

After some event or incident, this will be an example as well

**Discuss one type of asset that an organization might have.**

Database is one of the important asset that an organization might have. The databse contains all the past/present data, customer relationship data, future strategy and plan, research and developmetn data. The organization is totally dependent on the database as it provides various information to different department and personnel.

People and data / information / intellectual capital would be my two most important.

**When a security hardware device fails or a program aborts, which state should it go into?**

When the security hardware device fails or program aborts, it should go into the fail safe or fail-secure state. It put the system into the highest level of security even it is not operational.

**List two types of hardening techniques.**

The two types of hardening techniques are:

Password protected accounts and disable all unnecessary accounts

Disable all unnecessary services, which is equivalent to closing the ports

**List the steps of a DNS lookup**.

Below are the steps for the DNS lookup:

The computer searched in its local host table

If there is no entry in th local host table, then it goes to the local DNS server

If the local DNS server can't resolve the address than it send the request to the top-level domain DNS server

The top-level domain DNS server then sends back the IP address of the DNS server that contains the information about the requested address

The local DNS server then sends the request to that DNS server, which was received from the top-level DNS server.

This is how the DNS lookup is performed. The resolved address is then stored in the cache of the host and local DNS server for the future resolution.

**Discuss one security advantage to hosts running virtualization**.

One of the security advantages to host running virtualization is the virtual machines can be used to test the patch compatibility before installing the patches to the production environment. Similarly, the virtual machines can be used to test the security configurations, known as the security control testing. Multiple VMs can be run on the single host and one VM can virtually attack another VM on the same host to determine the vulnerabilities and security settings.

**List and describe the three service models of cloud computing.**

The three service models of the cloud computing are:

Software as a Service (SaaS): The user can access the vendor's software applications running on a cloud infrastructure. The vendor manages all these applications or softwares like installation, upgrade, configuration and so on.

Platform as a Service (PaaS): In this model the cloud computing vendor provides cloud infrastructures and the clients can install their own applicaions or softwares. The clients manage their installed applications or softwares not the cloud infrastructure like network, servers, OS, storage etc.

Infrastructure as a Service: This model provides greater control to the clients. The clients can install their own applications or softwares including operating systems. Though clients have some control over the installed softwares, applications, OS and storage, but the vendor will manages the cloud infrastructure.

**What is a VLAN? How is a VLAN created?**

VLAN is a Virtual Local Area Network that logically groups the devices/users. It segments the network and allow the logical grouping. VLAN can be created in switch and inter-VLAN routing is performed through routers.

**Describe at least three of the risks associated with BYOD.​**

The risk associated with the BYOD are:

The sensitive corporate data can be revealed among family members and friends.

Technical support staff may not provide support to different mobile devices with different operating systems.

Personal devices may be connected to the public Wi-fi or personal computers infected with malware and thus risking the corporate data stored on the mobile devices.

The corporate have limited access to the user device and it may be difficut to erase the corporate data from the user's mobile devices who was fired.

​**How might an attacker misuse a QR code?**

The attacker can advertise the QR code for reputable website, but include a malicious URL inside that will direct the user to the malicious website and download the malware.

**List at least three things that can be done in order to reduce the risk of theft or loss of a mobile device.**

Avoid using device on escalators, or near transit train doors.

Secure the mobile device by keeping it out of sight when travelling in a high-risk area.

Do not store mobile devices in lose clothes like in the pocket of jacket or hoodie.

Hold the mobile devices securely using both of your hands.

**Discuss the issues with the use of wireless networks, and what you can do about these. 20 points. I want a well-thought out answer.**

The primary concern with wireless network is the security vulnerabilities. Strong encryption and authentication should be used. There are ddifferent security protocol available in the market and we should always try to use the latest security protocol. Similarly, the wireless devices and access points must be updated frequetly with the latest software firmware.

The other issues with the wireless network is the weak Wi-Fi signal or interference. The interferring devices like microwave ovens, elevator motors, photocopy machine, cordless telephones etc needs to be kept away from the APs.

Similarly, it is not wise enough to access confedential information while in public Wi-Fi like at coffee shop, or airport and if we do need to then use VPN.

Response Feedback:

**Rogue APs? AP placement? Signal strength? SSID broadcasting?**

**Discuss the three areas of protection that are provided by IPsec.**

The three areas of protection provided by IPsec are:

Authentication: IPsec uses Authentication Header (AH) protocol that authenticates the source of the packets.

Confidentiality: IPsec uses Encapsulating Security Payload protocol to encrypt the packets and ensures no other parties were able to view the contents.

Key management: IPsec manages the key and it ensures that the keys are secure and not intercepted by unauthorized parties. The sending and receiving devices share a key using Internet Security Association and Key Management Protocol.

**What is a digital certificate? What is contained in a digital certificate? Where do you get one? For what would you use it?**

Selected Answer:

What is a digital certificate?

A digital certificate is the container for a public key and it is used to associate a user's identity to a public key, which is then digitally signed by a trusted third party.

What is contained in a digital certificate?

The digital certificate typically contains the following information:

Owner's name

Owner's email address/ Home address,

Owner's public key,

Name of the Issuer

Digital signature of the issuer

Serial number of the certificate

Expiration date of the public key

Where do you get one?

The digital certificate can be obtained from the Certificate Authority or Registration Authority.

For what would you use it?

Digital certificate is use to verify the owner of the public key. The ccertificate Authority or the Registration Authority verify the user and associte his/her identity to public key through the digital certificate.

**ACL**

An ACL is a list of "rules" telling the router what to do with certain types of packets. Each packet is evaluated against the ACL in place at the location where the packet currently is. The ACL is checked in order, from the first line downward. The first "rule" or line that matches the packet being evaluated is executed, so the ordering of rules is crucial.

When applying an ACL you must remember that from then on you have to specify everything for that interface/direction. There is an unwritten, implicit "Deny all" at the end of every ACL, so you have to make sure that your ACL contains at least 1 rule that allows traffic. Otherwise you will get nothing through the interface/direction.

**Steps in ACL configuration:**

Planning

Configuration

Assign the ACL to an interface (in or out direction)