

Security+ CertNotes

1. Three basic types of distributed trust models are:

- Hierarchical trust model: Here one root CA and one or more subordinate CAs will be present. The subordinate CAs provide redundancy and load balancing. The root CA is usually off-line. Here even if a subordinate CA is compromised, the root CA can revoke the subordinate CA, thus providing redundancy.
- Web of Trust: This is also called cross-certification model. Here CAs form peer-to-peer relationship. This model is difficult to manage as the number of CAs grow larger. This kind of trust relationship may happen when different divisions of a company has different CAs, and need to work together. Here CAs must trust one another.
- Bridge CA architecture: Bridge CA overcomes the complexity involved with Web of Trust model. Here Bridge CA act as the central co-ordinate point. All other CAs (known as principals) must trust only the Bridge CA.
If the CA's private key is compromised, certificates' private key is compromised, certificates issued by that CA issued by that CA are affected. This will lead to issuance of new certificates to all users, and registration. These problems can be overcome by use of a distributed trust model, in which multiple CAs are involved.

2. The following are the basic types of firewall architectures:

1. Bastion host
2. Screened host gateway
3. Screened subnet gateway or DMZ

3. Hash Algorithms: Hash algorithms produce a hash of a message and encrypt it. They use a mathematical formula for hashing, and it is extremely difficult to tamper with the message and still produce the same hash. Basically, Hashing enable a recipient to check whether a message is received intact without being tampered by a third party.

1. SHA (Secure Hashing Algorithms): There are several Secure Hashing Algorithms and they primarily differ in the hash length. They are SHA-1, SHA-256, SHA-384 and SHA-512. In SHA-1 the bit length is 160 bits, in SHA-256 it is 256 bits, for SHA-384, 384 bits and in SHA-512 it is 512 bits.
2. MD2, MD4, MD5 (Message Digest Series Algorithms): These are another type of hash algorithms. These algorithms were developed by Rivest. All three algorithms take a message of arbitrary length and produce a 128-bit message digest. MD2 is meant for 8 bit machines and MD4, MD5 are suitable for 32 bit machines. These algorithms are primarily

used for digital signature applications.

4. The two primary security services that are provided by IPSec are:

1. Authentication Header (AH), and
2. Encapsulating Security Payload

AH provides the authentication of the sender, and ESP provides encryption of the payload.

5. Some issues that need to be taken care of, while planning security policies are:

1. Due Care
2. Privacy
3. Separation of Duties
4. Need to Know
5. Password Management
6. Disposal Management
7. Human Resource Policies, and
8. Incident Management

6. Social engineering is a skill that an attacker uses to trick an innocent person such as an employee of a company into doing a favour. For example, the attacker may hold packages with both the hands and request a person with appropriate permission to enter a building to open the door. Social Engineering is considered to be the most successful tool that hackers use.

7. The following are the most commonly used access control mechanisms:

1. Mandatory Access Control (MAC): Here the access control is determined by the security policy of the system. The object owner or the user have almost no control over the resource.
2. Discretionary Access Control (DAC): Here the access control is determined by the owner of an object.
3. Role Based Access Control (RBAC): As the name suggests, the access to an object is determined by the role of an employee. Users are assigned roles first and then the permissions are assigned to roles.

8. DNS server uses UDP for name resolution uses port 53. Web server uses port 80. DHCP uses port 67 by default. FTP uses port 21.

9. Block cipher derives its name from the fact that a block of data is taken at a time to cipher.

10. Usually the user names and passwords are transmitted in plain text. But this kind of transmission

of authentication details is not secure. Any body with a packet sniffer can read the login and password. Kerberos is basically an authentication protocol that uses secret-key cryptography for secure authentication. In Kerberos, all authentication takes place between clients and servers. The name Kerberos comes from Greek mythology; it is the three-headed dog that guarded the entrance to Hades. It was developed by the Massachusetts Institute of Technology, USA

11. Biometrics is the ability measure physical characteristics of a human such as fingerprints, speech etc. These measured values are then used for authentication purpose. Given below are few of the measurable quantities:

- Fingerprint: Scans and matches finger print to a securely stored value.
- Voiceprint: Identifies a person by measuring speech pattern.
- Iris profile: Identifies a person by using Iris part of the eye.
- Signature: Matches an individual's signature with the stored value.
- Password is not a physical character of a human; any one can match a given password once it is known.

12. A token can be a physical device such as a smart card or an electronic process such as RSA's SecureID token. Tokens provide one of the most secure authentication environments, because typically a token is unique to a user, and it is difficult to spoof.

13. VPN (Short for Virtual Private Network) is private network formed using public Internet. It is formed between two hosts using tunneling protocols such as PPTP, L2TP, etc. Using VPN, you can connect two LANs in geographically distant locations together, as if they were located in the same building. The cost of connecting these LANs together is small since public Internet is used for providing the WAN link.

14. Buffer overflow occurs when the input is more than that allocated for that purpose. The system doesn't know what to do with the additional input, and it may result in freezing of the system, or sometimes to take control of the system by a hacker. By validating the inputs, it is possible to reduce this vulnerability to a great extent.

IP address check, and using short input fields are not a solution, and imposes restrictions on access and functionality. Avoiding email input doesn't help in solving the problem.

15. FTP transfers authentication information in clear text. The security concerns while using FTP also include buffer overflow, and anonymous access. However, the cache mining does not occur while using FTP.

16. Web servers are most prone to CGI script exploits, and buffer overflow attacks. CGI scripts run at server side performing a given functionality, such as writing to database or reading from database etc. Hackers may use the loopholes the scripts to hack in to the web server. Similarly, buffer-overflow can be used to run undesirable code on the server making it vulnerable.

War-driving is related to exploiting the vulnerabilities in wireless networks. Spam is primarily related to client side machines.

17. Non-repudiation ensures that the sender, as well as the receiver cannot refute having sent or received a message. For example, you receive an email from your perspective employer. By using an unsigned email, it might so happen that your employer later denies having sent any such email. Non-repudiation ensures that neither the sender nor the receiver can deny the transmission or the reception of a message respectively.

18. The VPN can be implemented in any of the following combinations:

- a. Gateway-to-gateway VPN
- b. Gateway-to-host VPN
- c. Host-to-gateway VPN
- d. Host-to-host VPN

The host-to-host configuration provides the highest security for the data. However, a Gate-to-Gateway VPN is transparent to the end users.

19. Hub: A hub is basically a multi-port repeater. When it receives a packet, it repeats that packet out each port. This means that all computers that are connected to the hub receive the packet whether it is intended for them or not. It's then up to the computer to ignore the packet if it's not addressed to it.

This might not seem like a big deal, but imagine transferring a 50 MB file across a hub. Every computer connected to the hub gets sent that entire file (in essence) and has to ignore it.

- Bridge: A bridge is a kind of repeater, but it has some intelligence. It learns the layer 2 (MAC) addresses of devices connected to it. This means that the bridge is smart enough to know when to forward packets across to the segments that it connects. Bridges can be used to reduce the size of a collision domain or to connect networks of differing media/topologies, such as connecting an Ethernet network to a Token Ring network.
- Switch: A switch is essentially a multi-port bridge. The switch learns the MAC addresses of each computer connected to each of its ports. So, when a switch receives a packet, it only forwards the packet out the port that is connected to the destination MAC address. Remember that a hub sends the packet out every port.
- Router: A router works at the logical layer of the IP stack. It is basically required to route packets from one network (or subnet) to another network (or subnet). In the given question, all the computers are within the same subnet and a router is inappropriate.
- Gateway: A gateway works at the top layers of the TCP/IP stack. For example, a Gateway may be used to facilitate communication between a Unix mail server and a Windows mail server.

20. NAT Filters and FireWalls:

- The Packet Filters work at Network Layer of OSI model.
- The Application Layer Proxy works at the Application Layer of OSI model
- Network Address Translation (NAT) is primarily used to hide internal network from external network, such as the Internet. A NAT basically translates the internal IP addresses to external IP addresses and vice-versa. This functionality assures that external users do not see the internal IP addresses, and hence the hosts.

- A Firewall implemented with stateful technology (like Checkpoint Firewall) works at all layers of the OSI model.

21. A company's security policy outlines the security measures to be taken. Implementing the security policy is the first thing that needs to be done.

22. DMZ is short for DeMilitarized Zone. If a company intends to host its own servers to be accessed from public Internet, a DMZ is most preferred solution. The network segment within the DMZ is secured by two firewalls, one interfacing with the public Internet, and the other interfacing the internal corporate network. Thus, a DMZ provides additional layer of security to internal corporate network. The type of servers that are hosted on DMZ may include web servers, email servers, file servers, DNS servers, etc.

23. According to the principle of least privilege, a user should be given only the minimum privileges that are required to do his/her works accurately and completely. Other choices are not appropriate.

24. Message Authentication Codes (MACs), also called "keyed hashes", are used to verify the authenticity of a message. Let us say, Jane (the sender of a message) and Mike (the recipient) share a secret key. Jane uses the message and the key to compute the MAC, and sends the MAC along with the message. When Mike receives the message, he computes the MAC, and then checks to see if his MAC matches Jane's. If it does, then he knows the message is from Jane and that nobody has changed it since she sent it.

25. Digital Signatures and Encryption:

- Digital signature ensures that the sender cannot repudiate having sent the message at a future date.
- Encryption ensures that the message cannot be read by any person who do not have matching key to decode the coded message
- Hashing ensures that the message is not tampered with, during transit or storage. Note that Hashing not necessarily encode or encrypt a message.

26. Secret-key encryption is also known as single-key or symmetric encryption. It involves the use of a single key that is shared by both the sender and the receiver of the message. Typically, the sender encrypts the message with a key and transmits the message to the recipient. The recipient then decrypts it by using a copy of the same key used to encrypt it.

27. Confidentiality ensures that a message is not disclosed to any unintended parties. Note that integrity is to do with the correctness of information, and authorization refers to privileges to access a given resource. Authentication is used in conjunction with validation of a user or a process to login.

28. Given below are some of the widely known password guessing methods:

1. dictionary
2. birthday
3. brute force
4. rainbow tables

1. dictionary: this is the method in which dictionary terms are used for guessing a password.
2. birthday: It takes advantage of probabilities, much like two people in a 50-person room shared the same birthday. With every person, the chances of two people having the same birth date increases. In the same way, when you start guessing the password, the chances of a hit keep increasing.
3. brute force: In a Brute Force attack, muscle (in this case, CPU and/or network muscle) is applied to break through a particular security mechanism, rather than using particular intelligence or logic. "Brute force" is most commonly applied to password guessing, taking advantage of computer power available to an attacker, to try every possible password value, until the right one is found. In cryptography, a brute-force attack is an attempt to recover a cryptographic key or password by trying every possible combination until the correct one is found. How quickly this can be done depends on the size of the key, and the computing resources applied.
4. rainbow tables: Rainbow tables are huge lists of keys or passwords. A password-guessing program uses these lists of keys or passwords rather than generating each key or password itself.

29. Computer based access controls prescribe not only who or what process may have access to a given resource, but also the type of access that is permitted. These controls may be implemented in the computer system or in external devices. Different types of access control are:

1. Mandatory access control
2. Discretionary access control
3. Rule based access control
4. Role based access control

Mandatory Access Control (MAC) secures information by assigning sensitivity labels on objects (resources) and comparing this to the level of sensitivity a subject (user) is operating at. MAC ensures that all users only have access to that data for which they have matching or greater security label (or security clearance). In general, MAC access control mechanisms are more secure than DAC. MAC is usually appropriate for extremely secure systems including multilevel secure military applications or mission critical data applications.

Discretionary Access Control (DAC): Discretionary Access Control (DAC) is a means of restricting access to information based on the identity of users and/or membership in certain groups. Access

decisions are typically based on the authorizations granted to a user based on the credentials he presented at the time of authentication (user name, password, hardware/software token, etc.). In most typical DAC models, the owner of information or any resource is able to change its permissions at his discretion. DAC has the drawback of the administrators not being able to centrally manage these permissions on files/information stored on the web server.

Role Based Access Control (RBAC): In Role-Based Access Control (RBAC), access decisions are based on an individual's roles and responsibilities within the organization. For instance, in a corporation, the different roles of users may include those such as chief executive, manager, executive, and clerk. Obviously, these members require different levels of access in order to perform their functions, but also the types of web transactions and their allowed context vary greatly depending on the security policy. In Role Based Access Control, the administrator sets the roles. Therefore, this type of access control is sometimes considered as a subset of MAC.

Rule Based Access Control (RBAC): The access to a resource in Rule Based Access Control is based a set of rules. ACLs (Access Control Lists) are used for this type of access control. In Rule Based Access Control, the administrator sets the rules. Therefore, this type of access control is sometimes considered as a subset of MAC.

30. 1. When a user first authenticates to Kerberos, he talks to the Authentication Service on the KDC to get a Ticket Granting Ticket (TGT). This ticket is encrypted with the user's password.

2. When the user wants to talk to a Kerberized service, he uses the TGT to talk to the Ticket Granting Service (TGS, also runs on the KDC). The TGS verifies the user's identity using the TGT and issues a ticket for the desired service.

The TGT ensures that a user doesn't have to enter in their password every time they wish to connect to a Kerberized service. The TGT usually expires after eight hours. If the Ticket Granting Ticket is compromised, an attacker can only masquerade as a user until the ticket expires.

The following are the important properties of Kerberos:

1. It uses symmetric encryption
2. Tickets are time stamped
3. Passwords are not sent over the network

31. The term "social engineering" refers to tricking someone into revealing useful information, such as a password. Social engineering can be used to collect any information an attacker might be interested in, such as the layout of your network, names and/or IP addresses of important servers, installed operating systems and software. The information is usually collected through phone calls or as new recruit or guest to your boss.

Phishing is the act of sending an e-mail to a user claiming to be a reputed organization (such as a bank) in an attempt to scam the user into providing information over the Internet. The e-mail directs the user to a Web site where they are prompted to provide private information, such as credit card, and

bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Vulnerability refers to what extent a system is prone to attack from a hacker.

Soft intrusion is a fictitious answer.

32. Viruses, worms, and Trojan horses are all harmful pieces of software. The way they differ is how they infect the computers, and spread.

- **Virus:** A computer virus attaches itself to a program or file so it can spread from one computer to another. Almost all viruses are attached to an executable file, and it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going.
- **Worm:** Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. The danger with a worm is its capability to replicate itself. Unlike Virus, which sends out a single infection at a time, a Worm could send out hundreds or thousands of copies of itself, creating a huge devastating effect.
- **Trojan Horse:** The Trojan Horse, at first glance appears to be a useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening it because it appears to be receiving legitimate software or file from a legitimate source.

33. Phishing is the practice of enticing unsuspecting Internet users to a fake Web site by using authentic-looking email with the legitimate organization's name, in an attempt to steal passwords, financial or personal information, or introduce a virus attack.

34. Simple Mail Transfer Protocol (SMTP), the main protocol used when sending email, does not include a way to authenticate where the email message originated. However, the mail server inserts a <Received:> header at the top of every email message. This gives us a message's route, making it possible to determine the origin of the message.

Email attachments from spammers usually contain malware, and one should never open such attachments.

35. A client authenticating itself to a server and that server authenticating itself to the client in such a way that both parties are assured of the others' identity is known as mutual or two-way authentication.

36. Zombies are malware that puts a computer under the control of a hacker. Hackers use zombies to launch DoS or DDoS attacks. The hacker infects several other computers through the zombie computer. Then the hacker sends commands to the zombie, which in turn sends the commands to slave computers. The zombie, along with slave computers start pushing enormous amount of useless data to

target computer, making it unable to serve its legitimate purpose. This type of attack is known as DDoS attack.

37. Kerberos uses port 88 by default. FTP uses port 21, https uses port 443, and SNMP uses port 161.

38. Any business continuity planning preferably include the following:

- a. Redundant network connectivity
- b. Clustering
- c. Fault tolerance using Raid or similar technique
- d. Facilities management

39. Security policy planning should include the following:

- a. Due care, acting responsibly and doing right thing.
- b. Privacy, letting the employees and administrator know of the privacy issues
- c. Separation of duties
- d. Need to know, providing employees only the information required to perform their role or duties.
- e. Password management, auditing the passwords
- f. Disposal and destruction
- g. Human rights policies, and
- h. Incident response, should take care of response to an act.

40. There are five types of extinguishers:

- a. Water
- b. Dry chemical
- c. Halon
- d. Carbon dioxide
- e. Foam

Water is used with Class A fires. Regular dry chemical extinguishers have a sodium bicarbonate base and are effective on Class B and C fires. Carbon Dioxide Extinguishers are used primarily on Class C fires and are also effective on Class B fires. Halon Extinguishers are best used on Class B or C fires. Foam extinguishers are less commonly used.

41. Disaster recovery plan is also called as business continuity plan or business process continuity plan. A DRP should include information security, asset security, and financial security plans.

42. Note that the divisions do not want the information to be made available to the group personnel only. A role based access control is suitable under this situation because it provides security, as well as flexibility. Here individual users are given privileges based on their respective roles in the organization rather than by name.

43. Kerberos require that the time sources are approximately in synchronization (within 5 minutes) with each other. However, with recent revisions of Kerberos software, this rule has become flexible.

44. The process of securing a computer system is called Hardening. There are several things that one needs to remember for hardening a PC. These include:

1. Removing non-essential programs, and services. These may provide back-doors for an attacker.
2. Installing an anti-virus package, and a spyware remover
3. Removing unnecessary protocols. If you are using only TCP/IP (required for connecting to the Internet), keep that protocol and remove all other protocols.
4. Disable guest account
5. Rename Administrator account
6. Enable auditing, so that you can view any logon attempts.
7. Installing latest patches, and service packs to operating system, and software.

45. A properly managed tape backups should include the following:

1. Regular backups according to a pre-determined plan
2. Verifying the backup tapes for integrity
3. Labeling tapes properly for easy and unique identification
4. Storing tapes securely at off-site location
5. Destroying data on old tapes before disposing of the same

46. The Layer 2 Tunnel Protocol (L2TP) is a standard that combines the best features of: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP does not provide information confidentiality by itself. IPSec is normally used in combination with L2TP for providing confidentiality of communication.

PGP is used primarily for securing email communications.

47. Advantages of fiber optic cable over CAT5 cable include the following:

- a. It provides communication over longer distance
- b. It is difficult to tap into a fiber optic cable
- c. It provides higher communication bandwidth
- d. It is more immune to external interference

However, from security point of view, two chief advantages are a. difficulty to tap, and b. immunity to external interference, which makes the communication not easily interruptible.

48. A few techniques used by IDS (Intrusion Detection Systems) include the following:

- a. Anomaly detection
- b. Signature detection
- c. Target monitoring, and

d. Stealth probes

Anomaly detection method establishes a baseline of normal usage patterns, and anything that widely deviates from the baseline is investigated for possible intrusion. An example of this would be if a user logs on and off of a machine 10 times a day instead of the normal once or twice a day.

Signature detection uses specifically known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures.

Target monitoring systems do not actively search for anomalies or misuse, but instead look for the modification of specified files.

49. In public key infrastructure:

A key is required to encode/decode a message, and the security of a message depends on the security of key.

A cipher text is the encoded message, and

A certificate is a digitally signed document by a trusted authority.

50. Staff training is the most effective tool for preventing attacks by social engineering.

51. A certificate revocation list (CRL) is a list of certificates, which have been revoked, and are no longer valid.

52. A back door is a program that allows access to the system without usual security checks. These are caused primarily due to poor programming practices.

The following are know back door programs:

1. Back Orifice: A remote administration program used to remotely control a computer system.
2. NetBus: This is also a remote administration program that controls a victim computer system over the Internet. Uses client –server architecture. Server resides on the victim’s computer and client resides on the hackers computer. The hacker controls the victim’s computer by using the client.
3. Sub7: This is similar to Back Orifice, and NetBus. Used to take control of victim’s computer over the Internet.

53. There are primarily three types of backups:

1. Full backup
2. Differential backup
3. Incremental backup

1. Full backup: Here all the data gets backed up. It usually involves huge amounts of data for large systems, and may take hours to complete. A full backup is preferred instead of incremental or differential backups where it is feasible. However, when there is large amount of data, full backup is done once in a while and incremental or differential backups are done in between. A backup plan is usually put in place prior to taking backup of data.

2. Differential backup: A differential backup includes all the data that has changed since last full

backup. The “differential backup” that was taken earlier (after the “full backup” but before the current “differential backup”) becomes redundant. This is because all changed data since last “full backup” gets backed up again.

3. Incremental backup: It includes all the data changed since last incremental backup. Note that for data restoration the full backup and all incremental backup tapes since last full backup are required. The archive bit is set after each incremental backup. Incremental backup is useful for backing up large amounts of data, as it backs up only the changes files since previous incremental backup.

54. There are primarily 5 classes of fire:

- Class 'A' Fire: Involves ordinary combustible materials such as wood, cloth and paper. Most fires are of this class.
- Class 'B' Fire: Involves flammable liquids or liquid flammable solids such as petrol, paraffin, paints, oils, greases and fat.
- Class 'C' Fire: Involves gases. Gaseous fires should be extinguished only by isolating the supply. Extinguishing a gas fire before the supply is off may cause an explosion.
- Class 'D' Fire: Involves burning metals. These should only be dealt with, by using special extinguishers, by personnel trained in the handling of combustible metals.
- Class 'F' Fire: Involves flammable liquids (Deep Fat Fryers)

The first three classes are most common.

55. Nonrepudiation is used to ensure that a sender cannot refuse later that he had not sent the message. A digital signature on the message ensures that the sender is the original sender of the electronic message.

56. Honeypot is the correct answer. Honeypots are designed such that they appear to be real targets to hackers. That is a hacker can not distinguish between a real system and a decoy. This enables lawful action to be taken against the hacker, and securing the systems at the same time.

57. CHAP (Challenge Handshake Authentication Protocol) works on point to point connections. It uses a three step process for authentication (excluding making the connection itself). If making the connection is also involved, it would be a 4 step process.

58. Social Engineering: Social Engineering exploits human behaviour. Nonrepudiation ensures that the sender of a message or contract can not refuse having sent the message or signed the contract at a later date. This is done by mean of digital signature. Retrenchment is not the correct answer. Separation of duties ensures that the vital activities are bifurcated among several individuals. This ensures that one or two individuals can not perform a fraud.

59. Vulnerability testing is part of testing corporate assets for any particular vulnerability. These may include:

1. Blind testing: Here the hacker doesn't have a prior knowledge of the network. It is performed from outside of a network.

2. Knowledgeable testing: Here the hacker has a prior knowledge of the network.
3. Internet service testing: It is a test for vulnerability of Internet services such as web service.
4. Dial-up service testing: Here the hacker tries to gain access through an organization's remote access servers.
5. Infrastructure testing: Here the infrastructure, including protocols and services are tested for any vulnerabilities.
6. Application testing: The applications that are running on an organization's servers are tested here.

Vulnerability assessment is part of an organization's security architecture.

60. VPN stands for Virtual Private Networking. PPTP (Point to Point Tunneling Protocol), and L2TP (Layer 2 Tunneling Protocol) are used for VPN.

61. Some of the features of Kerberos authentication system:

1. Uses client-server based architecture.
2. Kerberos server, referred to as KDC (Key Distribution Center) implements the Authentication Service (AS) and the Ticket Granting Service (TGS).
3. The term "application server" generally refers to Kerberized programs that clients communicate with using Kerberos tickets for authentication purpose. For example, the Kerberos telnet daemon (telnetd) is an example of an application server.

62. A biometric authentication depends on the physical characteristic of a human being. It is not something that can be remembered. Usually, bio authentication is very secure, though not widely used due to cost constraints.

63. The standard 802.1x corresponds to wireless network access protocols. Various wireless LAN protocols are given below:

1. IEEE 802.11 –supports data rate up to 2 Mbps in the 2.4 GHz frequency band.
2. IEEE 802.11a –supports data rates up to 54 Mbps in the 5 GHz frequency band.
3. IEEE 802.11b –supports data rates up to 11 Mbps in the 2.4 GHz frequency band.
4. IEEE 802.3 describes CSMA/CD Ethernet standard.
5. IEEE 802.5 describes Token Ring networks.
6. IEEE 802.4 is a standard for Token bus networks.

Note that IEEE 802.11x is the standard that pertains to wireless LANs.

64. IPSec uses authentication Header (AH), and Encapsulating Security Payload (ESP) protocols for transporting packets securely over the Internet. Note that PPTP and L2TP are tunneling protocols, where as IPSec provides strong encryption.

65. File Transfer Protocol (FTP) transfers files in unencrypted form. Even the authentication occurs in

clear text for FTP and Telnet. A hacker may gain access to an FTP server by exploiting this weakness.

66. Netstumbler can be used to sniff wireless networks during wardriving. The software tool provides several details of a wireless network such as SSID. PPTP is a tunneling protocol. WAP is a protocol, and not a software tool. ActiveX is a software component used with Microsoft programming languages such as Visual C.

67. Non-repudiation prevents either the sender or the receiver of messages from denying having sent or received a message.

68. A secure web page using SSL (Secure Socket Layer) starts with https instead of usual http. SSL uses asymmetric key with 40 or 128-bit cipher strength.

69. The host-to-host configuration provides the highest security for the data. However, a Gate-to-Gateway VPN is transparent to the end users.

70. Any software is inherently prone to vulnerabilities. Therefore, software manufacturers provide updates or patches to the software from time to time. These updates usually take care of any known vulnerabilities. Therefore, it is important to apply these updates.

Additional functionality is also one of the reasons for applying software updates. However, many times, it is not the compelling reason to apply the updates.

71. The Packet Filters work at Network Layer of OSI model.

- The Application Layer Proxy works at the Application Layer of OSI model
- Network Address Translation (NAT) is primarily used to hide internal network from external network, such as the Internet. A NAT basically translates the internal IP addresses to external IP addresses and vice-versa. This functionality assures that external users do not see the internal IP addresses, and hence the hosts.
- A Firewall implemented with stateful technology (like Checkpoint Firewall) works at all layers of the OSI model.

72. The employees of a Company typically use Intranet within the Company. The customers and vendors of the Company use Extranet. An Extranet is basically an extension of Intranet using public Internet. A typical use is when a Company has multiple vendors and do the order processing, and inventory control on-line.

Note that, on the other hand, Internet is accessible to everybody, i.e. general public.

The benefit of implementing Intranets and Extranets is security and customization. Intranets and Extranets are relatively safe because general public cannot access these networks. Intranets and Extranets are usually connected securely by means of Virtual Private Network (VPN).

73. IDS stands for Intrusion Detection System. There are primarily two types of IDSs. These are

Network based IDS (NIDS), and Host based IDS (HIDS). If the IDS monitors network wide communication, it is called Network based IDS, and if the IDS monitors security on a per host basis, it is called Host based IDS.

74. The first thing to be done when an intrusion is detected is to contain the damage. For example, if the intrusion is in the form of an unauthorized user, ensure that the user cannot access any network resource.

75. ISAKMP (Short for Internet Security Association and Key Management Protocol) defines payloads for exchanging key generation and authentication data.

76. A cryptographic hash function is a "one-way" operation. It is practically not possible to deduce the input data that had produced the output hash.

You can decrypt an encoded message using matching secret key. Similarly, Digital certificate is issued by a CA, and can be decrypted to find the contents of the certificate.

77. The disadvantages of using symmetric encryption over asymmetric encryption are given below:

1. Inability to support non-repudiation: Since both the sender and receiver use the same key, it is difficult to determine who is the sender, should a dispute arise.
2. Impractical for web commerce: Imagine thousands of customers buying goods and services over the Internet. If symmetric encryption standard is used, one unique private key-pair needs to be used for each user. It is therefore, impractical.
3. Another major difficulty is with the transmission of private key. With symmetric encryption, the private key needs to be transmitted to the other party for decryption, which may pose security risk.

78. Whether required or not, several services are installed by default. Disabling the services that are not required will ensure better security for the system.

79. A rootkit is a collection of tools that enable administrator-level access to a computer. Typically, a hacker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to gain root access to the computer and, possibly, other machines on the network.

A rootkit may consist of spyware and other programs that: monitor traffic, keystrokes, etc. using a "backdoor" into the system.

80. Defense against social engineering may be built by:

1. Including instructions in your security policy for handling it, and
2. Training the employees what social engineering is and how to deal with it.

The security policy should clearly state that no one is ever allowed to share his/her password with anyone else. Secondly, the security policy should state that the help desk can only change or assign a new password after positive identification of the individual requesting the information.

81. Some of the features of Kerberos authentication system:

1. Uses client-server based architecture.
2. Kerberos server, referred to as KDC (Key Distribution Center) implements the Authentication Service (AS), Ticket Granting Ticket and the Ticket Granting Service (TGS).
3. Uses symmetric encryption
4. Unlike other authentication protocols (FTP, PAP, etc. which transmits passwords over the network) passwords are not transmitted over the network.

82. Viruses, worms, and Trojan horses are all harmful pieces of software. The way they differ is how they infect the computers, and spread.

- **Virus:** A computer virus attaches itself to a program or file so it can spread from one computer to another. Almost all viruses are attached to an executable file, and it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going.
- **Worm:** Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. The danger with a worm is its capability to replicate itself. Unlike Virus, which sends out a single infection at a time, a Worm could send out hundreds or thousands of copies of itself, creating a huge devastating effect.
- **Trojan Horse:** The Trojan Horse, at first glance appears to be a useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening it because it appears to be receiving legitimate software or file from a legitimate source.
- **Rootkit:** It is a collection of tools that enable administrator-level access to a computer. Typically, a hacker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to gain root access to the computer and, possibly, other machines on the network.

83. Computer log files can be tampered with by a hacker to erase any intrusions. Computer logs can be protected using the following methods:

1. Setting minimal permissions
2. Using separate logging server
3. Encrypting log files
4. Setting log files to append only
5. Storing them on write-once media

Implementing all the above precautions ensures that the log files are safe from being tampered.

84. Phishing is the act of sending an e-mail to a user claiming to be a reputed organization (such as a bank) in an attempt to scam the user into providing information over the Internet. The e-mail directs the user to a Web site where they are prompted to provide private information, such as credit card, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Piggybacking is another type of social engineering. Here the intruder poses as a new recruit, or a guest to your boss. The intruder typically uses his social engineering skills to enter a protected premises on someone else's identity, just piggybacking on the victim.

85. Social engineering, and Trojan attack are two well-known problems associated with Discretionary Access Control (DAC).

86. TCP/IP Troubleshooting Utilities:

- NBTSTAT This utility displays current NetBIOS over TCP/IP connections, and display NetBIOS name cache.
- NETSTAT Displays current TCP/IP connections since the server was last booted.
- TRACERT Used to determine which route a packet takes to reach its destination from source.
- IPCONFIG Used to display Windows IP configuration information.
- NSLOOKUP This utility enables users to interact with a DNS server and display resource records.
- ROUTE Used to display and edit static routing tables.

87. RAID (short for Redundant Array of Inexpensive Disks) can be used to provide fault tolerance on a computer. There are several RAID levels such as RAID 1, RAID 5, etc. RAID 1 provides disk mirroring, where as RAID 5 provides striping with parity and minimum 3 disks are required for RAID 5.

Clustering is a technique where two or more computers are clustered and share the load. If one computer fails, the other computer's) take the load off the failed computer. Clustering is more expensive and requires two or more computers.

88. Acceptable use policy specifies what employees can do with their systems, and network access. The policy may put limits on personal use of resources, and resource access time.

89. It is recommended to store the backup tapes in a secure, physically distant location. This would take care of unforeseen disasters like natural disasters, fire, or theft. It is also important that the backup tapes are regularly verified for proper recovery in a test server, even though recovery is not really required at that time. Otherwise, it may so happen that you find a backup tape corrupt when it is really required.

90. A host based IDS should be place on a host computer such as a server. Network based IDS is typically placed on a network device such as a router.

91. Using Discretionary Access Control (DAC), the access rights for resources are controlled by the owner of a given resource.

92. For detecting spamware and virus, one need to install anti spamware, and anti virus programs. Installing the latest updates to Operating Systems will protect your system from exploits (like gaining back-door entry), but not necessarily from downloaded virus or spamware.

93. PGP uses public-key encryption for sending and receiving email messages. Diffie-Hellman and RSA algorithms are used for encryption/ decryption of PGP messages.

94. NAT (short for Network Address Translation) device changes the source IP address of a packet passing through it. Because of this, the destination host would not be able to receive the packets. The NAT devices at either side need to be configured so that it allows VPN packets through it.

95. A few techniques used by IDS (Intrusion Detection Systems) include the following:

- a. Anomaly detection
- b. Signature detection
- c. Target monitoring, and
- d. Stealth probes

96. SNMP is based on the manager/agent model. The manager runs on the server, and the agent runs on the client computers. Three important constituents of SNMP are a manager, an agent, and a database of management information. The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device(s) being managed. The manager and agent use a Management Information Base (MIB) and a set of commands to exchange information.

97. In Public Key Infrastructure parlance, the term Principal means an entity whose identity can be verified.

98. Encryption Schemes:

1. AES (Advanced Encryption Standard) is more secure than DES or 3DES.
2. AES is a symmetric block cipher that can encrypt (encipher) or decrypt (decipher) information
3. AES is based on Rijndael algorithm
4. PGP (Pretty Good Privacy) can use Diffie-Hellman or RSA algorithms, but not AES or DES.

99. All web applications such as Web servers, News servers, email servers etc. need to be configured as secure as possible. This can be achieved by

- Removing all unnecessary services. These are the services that are installed but not used. For example, you might have installed TFTP, but not using it. It is better to remove the application or service that is not used as it may provide an opportunity to a hacker to abuse the resource.
- Remove all unnecessary protocols: These are the protocols that are installed but not used. For example, you might have installed Novell Netware protocol but not necessary. It is preferable

to remove that protocol.

- Enable server and application logs: The logs provide an opportunity to look into the activity on the server over the past few hours or days. Check for any unusual activity such as failed login attempts etc.

100. The Internet architecture provides an unregulated network path to attack innocent hosts. Denial-of-service (DoS) attacks exploit this to target mission-critical services. DoS attacks, are explicit attempts to block legitimate users system access by reducing system availability. Any physical or host-based intrusions are generally addressed through hardened security policies and authentication mechanisms. Although software patching defends against some attacks, it fails to safeguard against DoS flooding attacks, which exploit the unregulated forwarding of Internet packets.

101. Authentication Types:

- Mutual authentication: Here both the server and client computers authenticate each other. This type of authentication is more secure than one-way authentication, where only the client is authenticated.
- Multifactor authentication: Here two or more number of authentication methods are used for granting access to a resource. Usually, it combines a password with that of a biometric authentication.
- Biometric authentication: Biometric authentication uses measurable physical attributes of a human being such as signature, fingerprint.
- CHAP: It is an authentication type that uses three-way handshake. The passwords are transmitted in encrypted form ensuring security. Compare this with PAP, which transmits passwords in clear text.

102. Sensitivity labels are associated with Mandatory Access Control (MAC).

103. A hacker begins a DDoS attack by exploiting a vulnerability in one computer system and making it the DDoS "master", also called as "zombie". It is from the zombie that the intruder identifies and communicates with other systems that can be compromised. The intruder loads hacking tools on the compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. This causes Distributed Denial of Service (DDoS) attack on the target computer.

104. Log Files Explained:

- Application log: The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. The developer decides which events to record.
- System log: The system log contains events logged by the Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined.

- Security log: The security log can record security events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.
- Antivirus log: Antivirus log analyzer can process log files from various antivirus packages and generate dynamic statistics from them, analyzing and reporting events.

105. “Single sign-on” enables one to use all the eligible services with one sign-in. Though other terms appear relevant, they are not widely used for describing this type of service.

106. Always try to download, and apply latest patches and service packs (if any) directly from the manufacturer’s website. Downloading from unreliable sources may compromise the system security.

107. SLA (Short for Service Level Agreement) is the formal negotiated document between two parties. It is a legal document that binds both the parties during the tenure of the agreement. DRP (stands for Disaster Recovery Planning), security audit, and invoice are not relevant answers.

108. A host based IDS should be place on a host computer such as a server. Network based IDS is typically placed on a network device such as a router.

109. In IP spoofing, the attacker uses somebody else’s IP address as the source IP address. Since routers forward packets based on the destination IP address, they simply forward the packets to the destination without verifying the genuineness of the source IP address.

110. A digital certificate is a credential issued by a trusted authority that binds you (and individual or an organization) to an identity that can be recognized and verified electronically by other agencies. Locally issued digital certificates are valid only within an organizations network (like intranet). Therefore, any secure pages or digital signatures containing local registration will not work on the Internet.

111. A personal firewall is software that resides on the end users computers. This is different from a regular firewall, in the sense that a personal firewall is geared to protect a single user computer.

112. Smurf attack is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system

113. DDoS, Short for Distributed Denial of Service, it is an attack where multiple compromised systems (which are usually infected with a Trojan) are used to send requests to a single system causing target machine to become unstable or serve its legitimate users.

114. PGP certificates differ from X.509 certificates in two ways:

1. PGP certificates are issued (signed) by normal people while the X.509 certificates must be issued by a professional CA, and
2. PGP implements a security fault tolerance mechanism, called the Web of Trust. Here an individual is allowed to sign and issue certificates to people they know.