ISM (UNIT– 2)

Q.1 what are the various uses of IDPS technologies?

Ans:

- IDPSs are primarily focused on identifying possible incidents.
- The IDPS could then report the incident to security administrators, they could initiate response to minimize the damage caused by the incident.
- Many IDPSs can also be configured to recognize violations of security policies.
- For example, some IDPSs can be configured with firewall, allowing them to identify network traffic that violates the organization's security .
- IDPSs can monitor file transfers and identify ones that might be suspicious, such as copying a large database onto a user's laptop.
- Other uses for IDPS are as follows:
    1. **Identifying security policy problems.**
        - An IDPS can provide some degree of quality control for security policy implementation, such as duplicating firewall rule sets and alerting when it sees network traffic that should have been blocked by the firewall.
    2. **Documenting the existing threat to an organization.**
        - IDPSs log information about the threats that they detect.
        - The information can also be used to educate management about the threats that the organization faces.
    3. **Deterring individuals from violating security policies.**
        - If individuals are aware that their actions are being monitored by IDPS technologies for security policy violations, they may be less likely to commit such violations because of the risk of detection.

Q. 2. What are the various functions of IDPS technologies?

Ans: In addition to monitoring and analyzing events to identify undesirable activity, all types of IDPS technologies typically perform the following functions:

1. Recording information related to observed events:

- Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.

2. Notifying security administrators of important observed events:

- This notification, known as an **alert**, occurs through any of several methods, including the following: e-mails, pages, messages on the IDPS user interface, etc.
- A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.

3. Producing reports:

- Reports summarize the monitored events or provide details on particular events of interest.
- Some IDPSs are also able to change their security profile when a new threat is detected.
  For example, an IDPS might be able to collect more detailed information for a particular session after malicious activity is detected within that session.

Q. 3 What are the common detection methodologies of IDPS?

Ans: IDPS technologies use many methodologies to detect incidents.

Most IDPS technologies use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection.

1. Signature-Based Detection:

- Signature-based detection is the process of comparing signatures against observed events to identify possible incidents.
  Example: A telnet attempt with a username of “root”, which is a violation of an organization’s security policy.
- Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats.
- Signature-based detection is the simplest detection method because it just compares the current unit of activity, such as a packet or a log entry, to a list of signatures using string comparison operations.
- Signature-based detection technologies have little understanding of many network or application protocols and cannot track and understand the state of complex communications.

2. Anomaly-Based Detection:

- Anomaly-based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.
- An IDPS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections, or applications.
- The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats.

- An initial profile is generated over a period of time (typically days, sometimes weeks) sometimes called a training period.
- Profiles for anomaly-based detection can either be static or dynamic.
- Once generated, a static profile is unchanged unless the IDPS is specifically directed to generate a new profile.
- A dynamic profile is adjusted constantly as additional events are observed.

3. Stateful Protocol Analysis:

- Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign (not harmful) protocol activity.
- For each protocol state against observed events to identify deviations.
- Stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used.
- The “stateful” in stateful protocol analysis means that the IDPS is capable of tracking the state of network, transport, and application protocols that have a notion of state.
- Stateful protocol analysis can identify unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command without first issuing a command upon which it is dependent.

Q. 4. What are the various types of IDPS technologies?

Ans: The IDPS technology are divided into the four groups based on the type of events that they monitor and the ways in which they are deployed:

1. Network-Based

- It monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.
- It is most commonly deployed at a boundary between networks, such as at border of firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks.

2. Wireless

- It monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves.
- It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP).

- It is most commonly deployed within range of an organization's wireless network to monitor it, but can also be deployed to locations where unauthorized wireless networking could be occurring.

3. Network Behavior Analysis (NBA)

- It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems).
- NBA systems are most often deployed to monitor flows on an organization's internal networks, and are also sometimes deployed where they can monitor flows between an organization's networks and external networks (e.g., the Internet, business partners' networks).

4. Host-Based

- It monitors the single host and the events occurring within that host for suspicious activity.
- Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

Q. 5 What are the typical components of IDPS System?

Ans: The typical components in an IDPS solution are as follows:

1. Sensor or Agent

- Sensors and agents monitor and analyze activity.
- The term sensor is typically used for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies.
- The term agent is typically used for host-based IDPS technologies.

2. Management Server

- A management server is a centralized device that receives information from the sensors or agents and manages them.
- Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot.
- Management servers are available as both appliance and software-only products.

- Some small IDPS deployments do not use any management servers and larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.

3. Database Server

- A database server is a repository for event information recorded by sensors, agents, and/or management servers.
- Many IDPSs provide support for database servers.

4. Console

- A console is a program that provides an interface for the IDPS's users and administrators.
- Console software is typically installed onto standard desktop or laptop computers.
- Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates.
- Some IDPS consoles provide both administration and monitoring capabilities.

Q. 6 **What are the typical components of network based IDPS System?**

Ans:

- A typical network-based IDPS is composed of sensors, one or more management servers, multiple consoles, and optionally one or more database servers.
- A network based IDPS sensor monitors and analyzes network activity on one or more network segments.
- Sensors are available in two formats:

1. Sensor

i. Appliance

- An appliance-based sensor is comprised of specialized hardware and sensor software.
- The hardware is typically optimized for sensor use including specialized NICs and NIC drivers for efficient capture of packets.
- Parts or all of the IDPS software might reside in firmware for increased efficiency.

ii. Software Only

- Some vendors sell sensor software without an appliance.
- Administrators can install the software onto hosts that meet certain specifications.
- The sensor software might include a customized OS.

2. Management Server

- A management server is a centralized device that receives information from the sensors or agents and manages them.
- Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot.
- Management servers are available as both appliance and software-only products.
- Some small IDPS deployments do not use any management servers and larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.

3. Database Server

- A database server is a repository for event information recorded by sensors, agents, and/or management servers.
- Many IDPSs provide support for database servers.

4. Console

- A console is a program that provides an interface for the IDPS's users and administrators.
- Console software is typically installed onto standard desktop or laptop computers.
- Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates.
- Some IDPS consoles provide both administration and monitoring capabilities.

Q. 7 List and explain various security capabilities of IDPS technologies.

Ans: Most IDPS technologies can provide a wide variety of security capabilities, divided into four categories: information gathering, logging, detection, and prevention.

1. Information Gathering Capabilities

- Some IDPS technologies offer information gathering capabilities, such as collecting information on hosts or networks from observed activity.
- Examples include identifying hosts, operating systems and applications that they use, and identifying general characteristics of the network.

2. Logging Capabilities

- IDPSs typically perform extensive logging of data related to detected events.

- Data fields commonly used by IDPSs include event date and time, event type, importance rating (e.g., priority, severity, impact, confidence), and prevention action performed.
- IDPS technologies typically permit administrators to store logs locally and send copies of logs to centralized logging servers.
- Generally, logs should be stored both locally and centrally to support the integrity and availability of the data.

3. Detection Capabilities

- IDPS technologies typically offer extensive, broad detection capabilities.
- Most products use a combination of detection techniques, which generally supports more accurate detection and more flexibility in tuning and customization.
- Examples of such capabilities are as follows:

a. Thresholds

- A threshold is a value that sets the limit between normal and abnormal behavior.
- Thresholds are most often used for anomaly-based detection and stateful protocol analysis.

b. Blacklists and Whitelists

- A blacklist is a list of discrete entities, such as hosts, TCP or UDP port numbers, ICMP types and codes, applications, usernames, URLs, filenames, or file extensions.
- Blacklists, also known as hot lists, are typically used to allow IDPSs to recognize and block activity that is highly likely to be malicious.
- Some IDPSs generate dynamic blacklists that are used to temporarily block recently detected threats.
- A whitelist is a list of discrete entities that are known to be benign.
- Whitelists and blacklists are most commonly used in signature-based detection and stateful protocol analysis.

c. Alert Settings

- Most IDPS technologies allow administrators to customize each alert type.
- an alert type include the following:

– Toggling it on or off

– Setting a default priority or severity level

– Specifying what information should be recorded and what notification should be used

– Specifying which prevention capabilities should be used.

d. Code Viewing and Editing

- Some IDPS technologies permit administrators to see some or all of the detection-related code.
- Viewing the code can help analysts to determine why particular alerts were generated, helping to validate alerts and identify false positives.
- The ability to edit all detection-related code and write new code is necessary to fully customize certain types of detection capabilities.

4. Prevention Capabilities

- IDPSs usually allow administrators to specify the prevention capability configuration for each type of alert.
- This usually includes enabling or disabling prevention, as well as specifying which type of prevention capability should be used.
- Some IDPS sensors have a learning or simulation mode that suppresses all prevention actions and instead indicates when a prevention action would have been performed.

Q. 8 what are the various types of sensors used in network based IDPS System?

Ans:

- A network based IDPS sensor monitors and analyzes network activity on one or more network segments.
- Sensors are available in two formats:

  1. Appliance
  - An appliance-based sensor is comprised of specialized hardware and sensor software.
  - The hardware is typically optimized for sensor use including specialized NICs and NIC drivers for efficient capture of packets.
  - Parts or all of the IDPS software might reside in firmware for increased efficiency.

  2. Software Only
  - Some vendors sell sensor software without an appliance.
  - Administrators can install the software onto hosts that meet certain specifications.
  - The sensor software might include a customized OS.

Q. 9 Explain packet filtering firewall technology.

Ans:

- The most basic feature of a firewall is the packet filter.
- Packet filters are not concerned about the content of packets.
- Their access control functionality is governed by a set of directives referred to as a rule set.
- Packet filtering capabilities are built into most operating systems and devices capable of routing.
- The most common example of a pure packet filtering device is a network router that employs access control lists.
- Firewalls with packet filters operate at the network layer. This provides network access control based on several pieces of information contained in a packet including:
    - The packet's source IP address—the address of the host from which the packet originated.
    - The packet's destination address—the address of the host the packet is trying to reach.
- Filtering inbound traffic is known as ingress filtering. Outgoing traffic can also be filtered, a process referred to as egress filtering.
- Here, organizations can restrict on their internal traffic, such as blocking the use of FTP servers or preventing denial of service (DoS) attacks from being launched from within the organization against outside entities.
- Some packet filters can specifically filter packets that are fragmented.
- Some firewalls can reassemble fragments before passing them to the inside network, although this requires additional firewall resources, particularly memory.

Q.10 Explain the dedicated proxy server, application proxy server firewall technology.

Ans:

- **Application-Proxy Gateways**
    - An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality.
    - These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them.
    - Each successful connection attempt actually results in the creation of two separate connections—one between the client and the proxy server, and another between the proxy server and the true destination.
    - In addition to the rule set, some proxy agents have the ability to require authentication of each individual network user.
    - Firewalls with application-proxy gateways can also have several disadvantages when compared to packet filtering and stateful inspection.

- First, because of the “full packet awareness” of application-proxy gateways, the firewall spends much more time reading and interpreting each packet.
- Application-proxy gateways tend to be limited in terms of support for new network applications and protocols.

- **Dedicated Proxy Servers**
  - Dedicated proxy servers have limited firewalling capabilities
  - Dedicated proxy servers are application-specific, and some actually perform analysis and validation of common application protocols such as HTTP.
  - This server would perform filtering or logging operations on the traffic, then forward it to internal systems.
  - A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and pass it to the firewall for outbound delivery.
  - Dedicated proxy servers are generally used to decrease firewall workload and conduct specialized filtering and logging that might be difficult to perform on the firewall itself.

Q. 11 Explain how firewall act as network address translators.

Ans:

- Most firewalls can perform NAT, which is sometimes called port address translation (PAT) or network address and port translation (NAPT).
- Typically, a NAT acts as a router that has a network with private addresses on the inside and public address on the outside.
- The way a NAT performs this many-to-one mapping varies between implementations.
- Hosts on the inside network initiating connections to the outside network because the NAT to map the source port of the connection to a different source port that is controlled by the NAT.
- The NAT uses this source port number to map connections from the outside back to the host on the inside.
- Hosts on the outside of the network cannot initiate contact with hosts on the inside network.
- In some firewalls, the NAT can be configured to map a particular destination port on the NAT to a particular host on the inside of the NAT.
- NAT is not part of the security functionality of a firewall, they interact with the firewall’s security policy.

Q. 12 Explain stateful inspection.

Ans:

- Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state.
- Stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule.
- Unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information.
- Stateful inspection in a firewall examines certain values in the TCP headers to monitor the state of each connection.
- Each new packet is compared by the firewall to the firewall's state table to determine if the packet's state contradicts its expected state.
- If a device on the internal network (shown here as 192.168.1.100) attempts to connect to a device outside the firewall (192.0.2.71), the connection attempt is first checked to see if it is permitted by the firewall rule set. If it is permitted, an entry is added to the state table that indicates a new session is being initiated,

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established

Figure: State table

Q. 13 Write short note on application firewalls.

Ans:

- Application firewalls can identify unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command that was not preceded by another command on which it is dependent.
- These suspicious commands often originate from buffer overflow attacks, DoS attacks, malware, and other forms of attack carried out within application protocols such as HTTP.
- Common feature is input validation for individual commands, such as minimum and maximum lengths for arguments.

- Application firewalls are available for many common protocols including HTTP, database (such as SQL), email (SMTP, Post Office Protocol [POP], and Internet Message Access Protocol [IMAP]), voice over IP (VoIP), and Extensible Markup Language (XML).
- Some application firewalls involves enforcing application state machines, which are essentially checks on the traffic's compliance.

Q.14 Write short note on Application-Proxy Gateways & Dedicated Proxy Servers

Ans:

- **Application-Proxy Gateways**
  - An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality.
  - These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them.
  - Each successful connection attempt actually results in the creation of two separate connections—one between the client and the proxy server, and another between the proxy server and the true destination.
  - In addition to the rule set, some proxy agents have the ability to require authentication of each individual network user.
  - Firewalls with application-proxy gateways can also have several disadvantages when compared to packet filtering and stateful inspection.
  - First, because of the "full packet awareness" of application-proxy gateways, the firewall spends much more time reading and interpreting each packet.
  - Application-proxy gateways tend to be limited in terms of support for new network applications and protocols.

- **Dedicated Proxy Servers**
  - Dedicated proxy servers have limited firewalling capabilities
  - Dedicated proxy servers are application-specific, and some actually perform analysis and validation of common application protocols such as HTTP.
  - This server would perform filtering or logging operations on the traffic, then forward it to internal systems.
  - A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and pass it to the firewall for outbound delivery.
  - Dedicated proxy servers are generally used to decrease firewall workload and conduct specialized filtering and logging that might be difficult to perform on the firewall itself.

Q.15 Write short note on Web Application Firewalls & Firewalls for Virtual Infrastructures.

Ans:

- **Web Application Firewalls**
  - The HTTP protocol used in web servers has been exploited by attackers in many ways.
  - The attacker can place malicious software on the computer of someone browsing the web.
  - Many of these exploits can be detected by specialized application firewalls called **web application firewalls** that reside in front of the web server.
  - Web application firewalls are a relatively new technology, as compared to other firewall technologies.
  - The type of threats that they mitigate are still changing frequently because they are put in front of web servers to prevent attacks on the server.

- **Firewalls for Virtual Infrastructures**
  - Many virtualization solutions allow more than one operating system to run on a single computer simultaneously.
  - This has become popular recently because it allows organizations to make more efficient use of computer hardware.
  - Network activity that passes directly between virtualized operating systems within a host cannot be monitored by an external firewall.
  - However, some virtualization systems offer built-in firewalls or allow third-party software firewalls to be added as plug-ins.
  - Using firewalls to monitor virtualized networking is a relatively new area of firewall technology, and it is likely to change significantly as virtualization usage continues to increase.

Q.16 State the Limitations of Firewall Inspection.

Ans:

- Firewalls can only work effectively on traffic that they can inspect.
- A firewall that cannot understand the traffic flowing through it will not handle that traffic properly. For example, allowing traffic that should be blocked.
- Firewalls also cannot read application data that is encrypted, such as email that is encrypted using the S/MIME or OpenPGP protocols, or files that are manually encrypted.
- Some firewalls is not understanding traffic that is tunneled, even if it is not encrypted.

- For example, IPv6 traffic can be tunneled in IPv4 in many different ways. The content may still be unencrypted, but if the firewall does not understand the particular tunneling mechanism used, the traffic cannot be interpreted.

Q.17 Write short note on VPN

Ans:

- Firewall devices at the edge of a network are sometimes required to do more than block unwanted traffic.
- A common requirement for these firewalls is to encrypt and decrypt specific network traffic flows between the protected network and external networks. This nearly always involves virtual private networks (VPN).
- VPNs are most often used to provide secure network communications across untrusted networks.
- Two common choices for secure VPNs are IPsec and Secure Sockets Layer (SSL)/Transport Layer Security (TLS).
- The VPN functionality is often part of the firewall itself.
- The two most common VPN architectures are gateway-to-gateway and host-to-gateway.

1. Gateway-to-gateway Architectures

- Gateway-to-gateway architectures connect multiple fixed sites over public lines by using VPN gateways.
- For example, to connect branch offices to an organization's headquarters.
- A VPN gateway is usually part of another network device such as a firewall or router.

2. Host-to-gateway Architectures

- It provides a secure connection to the network for individual users, usually called **remote users**, who are located outside of the organization.
- Here, a client on the user machine negotiates the secure connection with the organizations by using organization VPN gateway.
- Host-to-gateway VPNs allow the firewall administrator to decide which users have access to which network resources.

Q.18 Explain various network layouts with firewall implementation.

Ans:

- A typical network layout with a hardware firewall device acting as a router.

- The unprotected side of the firewall connects to the single path labeled “WAN,” and the protected side connects to three paths labeled “LAN1,” “LAN2,” and “LAN3.”
- The firewall acts as a router for traffic between the wide area network (WAN) path and the LAN paths. One of the LAN paths also has a router.

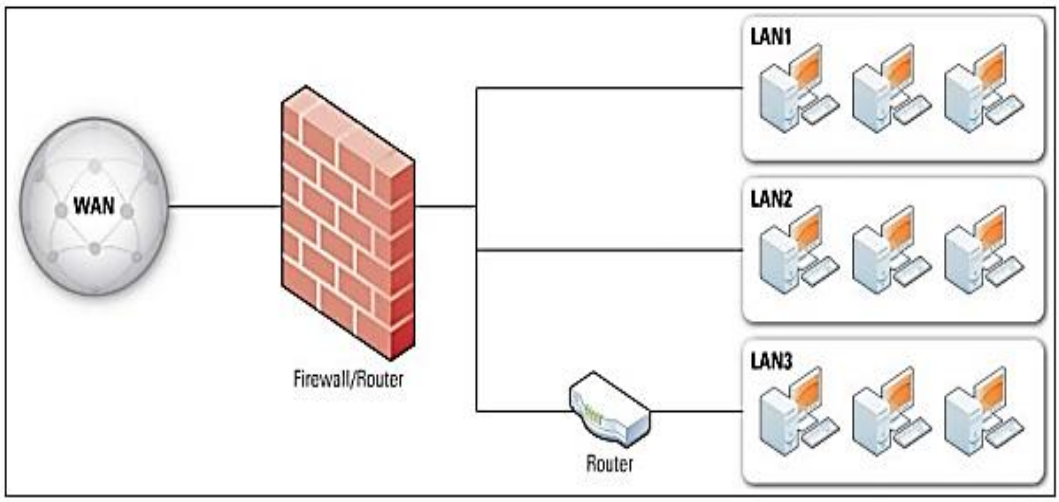

Figure: Simple Routed Network with Firewall Device

- Many hardware firewall devices have a feature called demilitarized zones (DMZ).
- DMZ are usually interfaces on a routing firewall that are similar to the interfaces found on the firewall’s protected side.
- The major difference is that traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied.
- Traffic from the Internet goes into the firewall and is routed to systems on the DMZ.
- Traffic between systems on the DMZ and systems on the protected network goes through the firewall, and can have firewall policies applied.

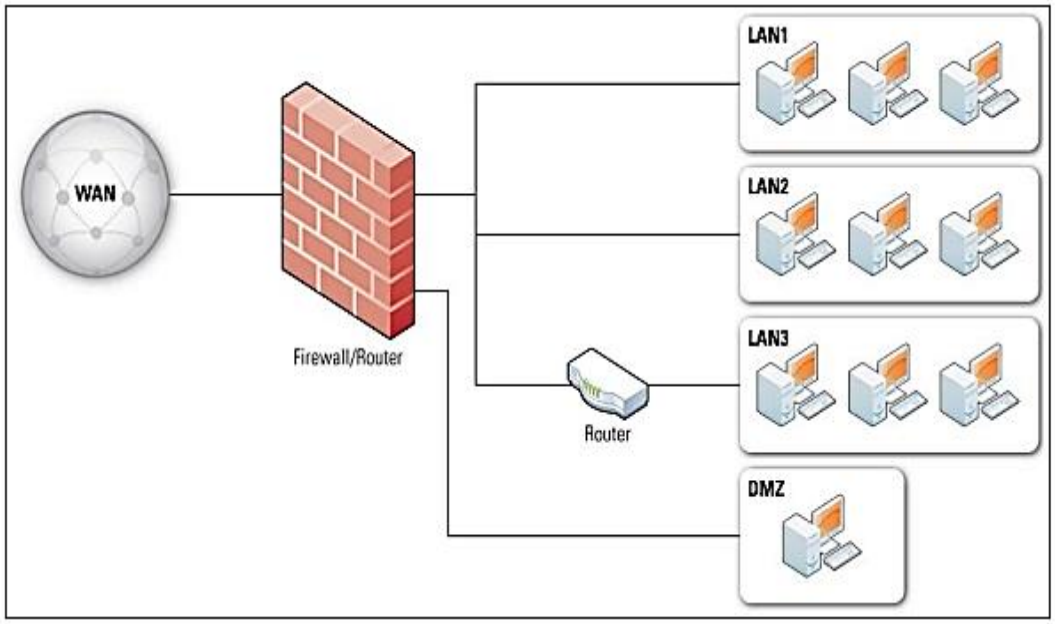

Figure: Firewall with a DMZ

Q.19 what are the various policies based on ip addresses

Ans:

- Firewall policies should only permit appropriate source and destination IP addresses to be used.
- Policies based on ip addresses are as follows:
  - Traffic with invalid source or destination addresses should always be blocked regardless of the firewall location...
    Examples of relatively common invalid IPv4 addresses are 127.0.0.0 to 127.255.255.255.
  - Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic should be blocked at the network perimeter. This traffic is often caused by malware, spoofing, denial of service attacks.
  - Traffic with a private destination address for incoming traffic or source address for outgoing traffic should be blocked at the network perimeter. Perimeter devices can perform address translation services to permit internal hosts with private addresses to communicate through the perimeter, but private addresses should not be passed through the network perimeter.
  - Outbound traffic with invalid source addresses should be blocked. Blocking this type of traffic at an organization's firewall helps reduce the effectiveness of these attacks.

- Incoming traffic with a destination address of the firewall itself should be blocked unless the firewall is offering services for incoming traffic that require direct connections—for example, if the firewall is acting as an application proxy.

Q.20 what are the various policies based on protocols.

Ans: Policies based on protocol are as follows:

1. TCP and UDP

- Application protocols can use TCP, UDP, or both, depending on the design of the protocol.
- An application server typically listens on one or more fixed TCP or UDP ports.
- Some applications use a single port, but many applications use multiple ports. For example, although SMTP uses TCP port 25 for sending mail, it uses TCP port 587 for mail submission.
- Default policies should be used for incoming TCP and UDP traffic.
- **Less stringent** policies are generally used for outgoing TCP and UDP traffic because most organizations permit their users to access a wide range of external applications located on millions of external hosts.

2. ICMP

- Some firewall policies block all ICMP traffic, but this often leads to problems with diagnostics and performance.
- For ICMP in IPv4, ICMP type 3 messages should not be filtered because they are used for important network diagnostics.
- For ICMP in IPv6, many types of messages must be allowed in specific circumstances to enable various IPv6 features.
- ICMP within an organization's network generally should not be blocked by firewalls that are not at the perimeter of the network.

3. IPsec Protocols

- The ESP and AH protocols are used for IPsec VPNs, and a firewall that blocks these protocols will not allow IPsec VPNs to pass.
- While blocking ESP can perform encryption to protect sensitive data.
- Organizations that allow IPsec VPNs should block ESP and AH except to and from specific addresses on the internal network—those addresses belong to IPsec gateways that are allowed to be VPN endpoints.
- Enforcing this policy will require people inside the organization to obtain the appropriate policy approval to open ESP and/or AH access to their IPsec routers.

Q.21 what are the various policies based on applications, user identity & Network Activity.

Ans:

- **Policies Based on Applications**
  - The application-based approach provides an additional layer of security for incoming traffic by validating some of the traffic before it reaches the desired server.
  - In some cases, an application firewall or proxy can remove traffic that the server might not be able to remove on its own because it has greater filtering capabilities.
  - An application firewall or proxy also prevents the server from having direct access to the outside network.
  - Policies based on application are as follows:
    - Is a suitable application firewall available?
    - Is the server already sufficiently protected by existing firewalls?
    - Can the main server remove malicious content as effectively as the application firewall or proxy?
- **Policies Based on User Identity**
  - Many firewall technologies can see these identities and therefore enact policies based on user authentication.
  - One of the most common ways to enforce user identity policy at a firewall is by using a VPN.
  - Both IPsec VPNs and SSL VPNs have many ways to authenticate users, such as with secrets that are provisioned on a user-by-user basis with multi-factor authentication (e.g., time-based cryptographic tokens protected with PINs), or with digital certificates controlled by each user.
  - NAC has also become a popular method for firewalls to allow or deny users access to particular network resources.
- **Policies Based on Network Activity**
  - Many firewalls allow the administrator to block established connections after a certain period of inactivity.
  - For example, if a user on the outside of a firewall has logged into a file server but has not made any requests during the past 15 minutes, the policy might be to block any further traffic on that connection.
  - Time-based policies are useful in thwarting attacks caused by a logged-in user walking away from a computer and someone else sitting down and using the established connections.
  - However, these policies can also be bother for users who make connections but do not use them frequently.

- Firewall policy based on network activity is one that redirects traffic if the rate of traffic matching the policy rule is too high.
- Another policy might be to drop incoming ICMP packets if the rate is too high.

Q.22 Explain with diagram IT security requirements.

Ans: There are types of IT security requirement are as follows:

1. Security Solutions

- Security solutions should be designed with two focus area; functional requirement of the solution area and assurance requirement of the functional solution is working correctly.
- Solution is not completed unless it addresses both of these area.

2. Functional Requirement

- Functional Requirement are the thing that considering security controls.
- The risk assessment provide the consideration for functional controls are as follows:
  - They should be layered and meet a specific security requirement.
  - They should not be depend on another control.
  - They should fail safe that is in the event of control they maintain the security of system.

3. Assurance requirement

- It conforms that the security solution are selected properly, performing as intended, and are having the desired effect.
- Many assurance mechanism reviewed within their respective domains i.e. IDS's, Audit logs, BCP tests etc.

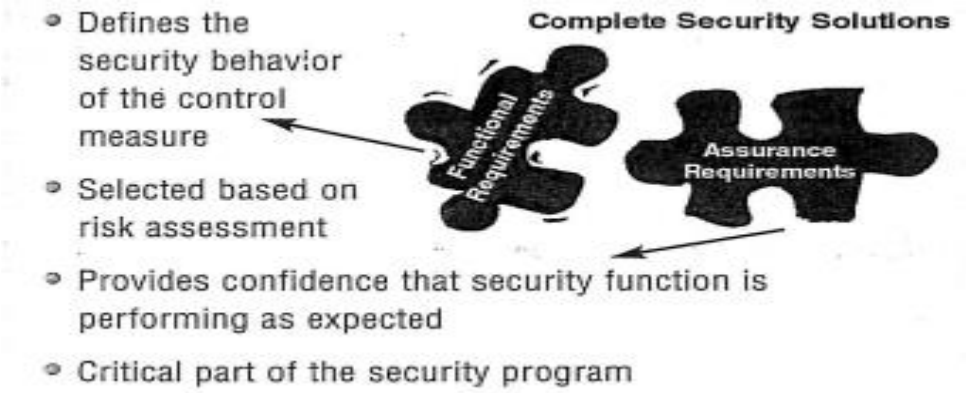

Figure: IT Security Requirement

Q.23 what should be considered in the planning stages of a Web server?

Ans: In the planning stages of a Web server, the following items should be considered

- Identify the purpose(s) of the Web server
  - What information categories will be stored on the Web server?
  - What information categories will be processed on or transmitted through the Web server?
  - What are the security requirements for this information?
  - Will any information be retrieved from or stored on another host (e.g., back-end database, mail server)?
  - What other services will be provided by the Web serve?
  - What are the security requirements for these additional services?
- Identify the network services that will be provided on the Web server, that provided by following protocols:
  - HTTPS
  - Internet Caching Protocol (ICP)
  - Hyper Text Caching Protocol (HTCP)
  - Web Cache Coordination Protocol (WCCP)
  - Database services (e.g., open Database Connectivity [ODBC]).
- Identify any network service software, both client and server, to be installed on the Web server and any other support servers.
- Identify the users or categories of users of the Web server.
- Decide if and how users will be authenticated and how authentication data will be protected.
- Determine how the Web server will be managed
- Are the appropriate physical security protection mechanisms in place?
  - Locks
  - Card reader access
  - Security guards
  - Physical IDSs (e.g., motion sensors, cameras).
- Are there appropriate environmental controls so that the necessary humidity and temperature are maintained?
- is there a backup power source? For how long will it provide power?

Q.24 what are the steps for securely installing web server?

Ans: During the installation of the Web server, the following steps should be performed:

- Install the Web server software either on a dedicated host or on a dedicated guest OS if virtualization is being employed.
- Apply any patches or upgrades to correct for known vulnerabilities.

- Create a dedicated physical disk or logical partition for Web content.
- Remove or disable all services installed by the Web server application but not required (e.g., gopher, FTP, remote administration).
- Remove or disable all unneeded default login accounts created by the Web server installation.
- Remove all manufacturers' documentation from the server.
- Remove all example or test files from the server, including scripts and executable code.
- Apply appropriate security template or hardening script to server.
- Reconfigure HTTP service banner not to report Web server and OS type and version.

Q.25 Sate and explain any 4 Wireless Standards

Ans:

1. Wireless personal area networks (WPAN)

- A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables.
- Examples of WPAN standards include the following:
  - **IEEE 802.15.1 (Bluetooth):** This WPAN standard is designed for wireless networking between small portable devices.
  - **IEEE 802.15.3 (High-Rate Ultra wideband; WiMedia, Wireless USB):** This is a low-cost, low power consumption WPAN standard that uses a wide range of GHz frequencies to avoid interference with other wireless transmissions.
  - **IEEE 802.15.4 (Low-Rate Ultra wideband; ZigBee):** This is a simple protocol for lightweight WPANs.9 It is most commonly used for monitoring and control products, such as climate control systems and building lighting.

2. Wireless local area networks (WLAN)

- IEEE 802.11 is the dominant WLAN standard.
- High Performance Radio Local Area Network (HIPERLAN) WLAN standard that transmits data in the 5 GHz band and operates at data rates of approximately 23.5 Mbps.1.

3. Wireless metropolitan area networks (WMAN)

- Many WMAN implementations provide wireless broadband access to customers in metropolitan areas.

- For example, IEEE 802.16e (better known as WiMAX) is a WMAN standard that transmits in the10 to 66 GHz band range.

4. Wireless wide area networks (WWAN)

- Networks that connect individuals and devices over large geographic areas, often globally.
- WWANs are typically used for cellular voice and data communications, as well as satellite communications.

Q.26 State IEEE 802.11 Network Components and explain its Architectural Models.

Ans: IEEE 802.11 has two fundamental architectural components, as follows:

1. Station (STA)

- A STA is a wireless endpoint device. Typical examples of STAs are laptop computers, personal digital assistants (PDA), mobile phones, and other consumer electronic devices with IEEE 802.11 capabilities.

2. Access Point (AP)

- An AP logically connects STAs with a distribution system (DS), which is typically an organization's wired infrastructure.
- APs can also logically connect wireless STAs with each other without accessing a distribution system.

➢ The IEEE 802.11 standard also defines the following two WLAN design structures:

1. Ad Hoc Mode

- The ad hoc mode does not use APs.
- This mode of operation, also known as peer-to-peer mode, is possible when two or more STAs are able to communicate directly to one another.
- One of the key advantages of ad hoc WLANs is that theoretically they can be formed anytime and anywhere and allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance.

Figure: IEEE 802.11 Ad Hoc Mode

2. Infrastructure Mode

- In infrastructure mode, an IEEE 802.11 WLAN comprises one or more Basic Service Sets (BSS), the basic building blocks of a WLAN.
- A BSS includes an AP and one or more STAs. The AP in a BSS connects the STAs to the DS.
- The DS is the means by which STAs can communicate with the organization's wired LANs and external networks such as the Internet.

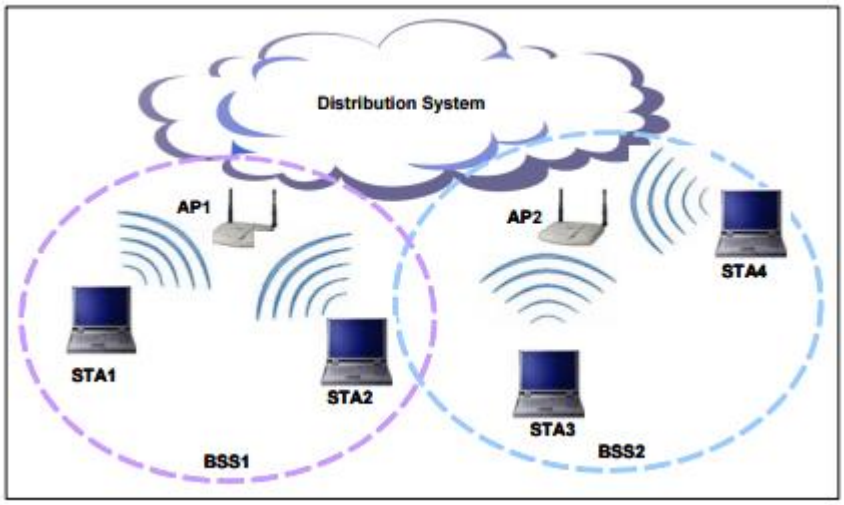

Figure: IEEE 802.11 Infrastructure Mode

- The DS and use of multiple BSSs and their associated APs allow for the creation of wireless networks of arbitrary size and complexity. In the IEEE 802.11 specification, this type of multi-BSS network is referred to as an extended service set (ESS).

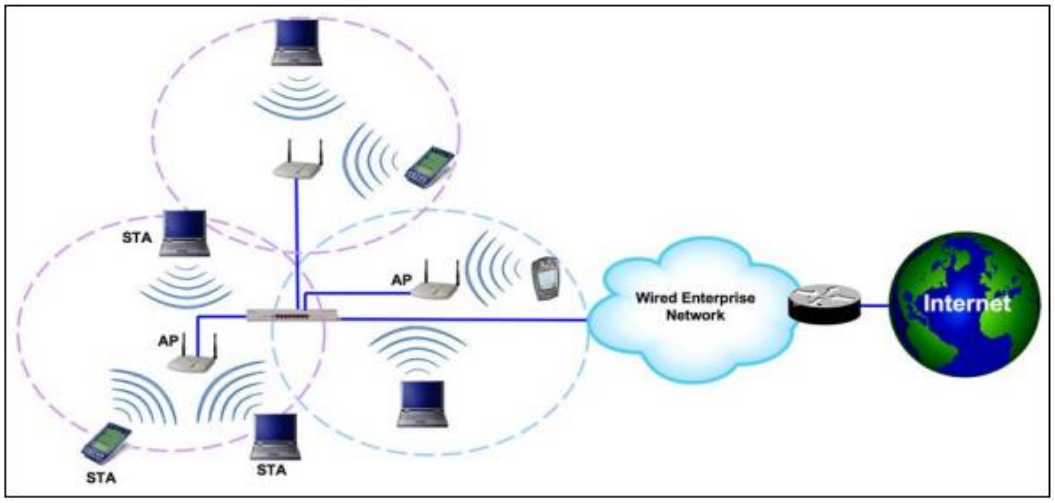

Figure: Extended Service Set in an Enterprise

Q.27 what are the various types of authentic methods implemented in IEEE 802.11 security?

Ans: The IEEE 802.11 defines two authentic methods are as follows:

1. Open System Authentication

- Open system authentication is null authentication mechanism that does not provide true identity verification.
- In practice, a STA is authenticated to an AP simply by providing the following information:

i. Service Set Identifier (SSID) for the AP

- The SSID is a name assigned to a WLAN.
- It allows STAs to distinguish one WLAN from another.
- SSIDs are broadcast in plaintext in wireless communications, so an eavesdropper can easily learn the SSID for a WLAN.
- However, the SSID is not an access control feature, and was never intended to be used for that purpose.

ii. Media Access Control (MAC) address for the STA

- A MAC address is a (hopefully) unique 48-bit value that is permanently assigned to a particular wireless network interface.
- Many implementations of IEEE 802.11 allow administrators to specify a list of authorized MAC addresses.

- The AP will permit devices with those MAC addresses only to use the WLAN. This is known as MAC address filtering.

- Open system authentication does not provide reasonable assurance of any identities, and can be misused easily to gain unauthorized access to a WLAN.

2. Shared key authentication

- Shared key authentication was supposed to be more robust than open system authentication and equally insecure also.
- Shared key authentication is based on a secret cryptographic key known as a Wired Equivalent Privacy (WEP) key; this key is shared by legitimate STAs and APs.
- Shared key authentication uses a simple challenge-response scheme based on whether the STA seeking WLAN access knows the WEP key.
- The STA initiates an Authentication Request with the AP, and the AP generates a random 128-bit challenge value and sends it to the STA.
- Using the WEP key, the STA encrypts the challenge and returns the result to the AP.
- The AP decrypts the result using the same WEP key and allows the STA access only if the decrypted value is the same as the challenge.
- Shared key authentication is still weak because the AP is not authenticated to the STA, so there is no assurance that the STA is communicating with a legitimate AP.

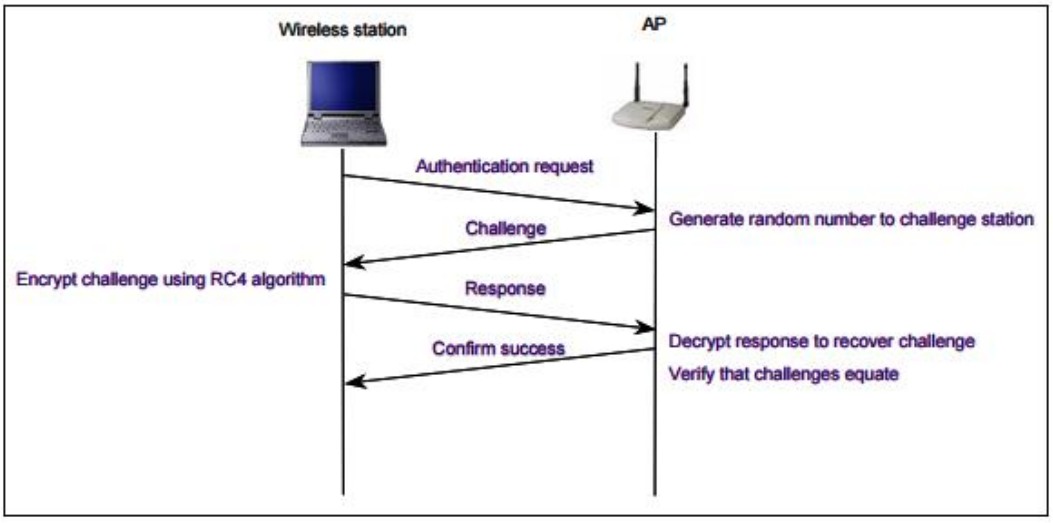

Figure: Shared Key Authentication Message Flow

Q.28 Write short note on IEEE 802.11i security.

Ans:

- The IEEE 802.11i standard is the sixth amendment to the baseline IEEE 802.11 standards.
- It includes many security enhancements that implement mature and proven security technologies.
- For example, IEEE 802.11i references the Extensible Authentication Protocol (EAP) standard, which is a means for providing mutual authentication between STAs and the WLAN infrastructure.
- The IEEE 802.11i specification introduces the concept of a Robust Security Network (RSN).
- An RSN is defined as a wireless security network that only allows the creation of Robust Security Network Associations (RSNA).
- An RSNA is a logical connection between communicating IEEE 802.11 entities established through the IEEE 802.11i key management scheme, called the **4-Way Handshake.**
- 4-way handshake is a protocol that validates that both entities share a pairwise master key (PMK) and confirms the selection and configuration of data confidentiality and integrity protocols.
- The PMK serves as the basis for the IEEE 802.11i data confidentiality and integrity protocols that provide enhanced security over the flawed WEP.
- The IEEE 802.1X standard, which is specified by the IEEE 802.11i amendment.
- The IEEE 802.1X standard defines several terms related to authentication. The authenticator is an entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.
- For example, the AP in Figure serves as an authenticator.
- The STA may be viewed as a supplicant which being authenticated.
- The authentication server (AS) is an entity that provides an authentication service to an authenticator.
- AS determines supplicant is authorized to access the services provided by the authenticator.
- The AS provides these authentication services and delivers session keys to each AP in the wireless network.
- Each STA either receives session keys from the AS or derives the session keys itself.
- The AS either authenticates the STA and AP itself, or provides information to the STA and AP so that they may authenticate each other. The AS typically lies inside the DS.

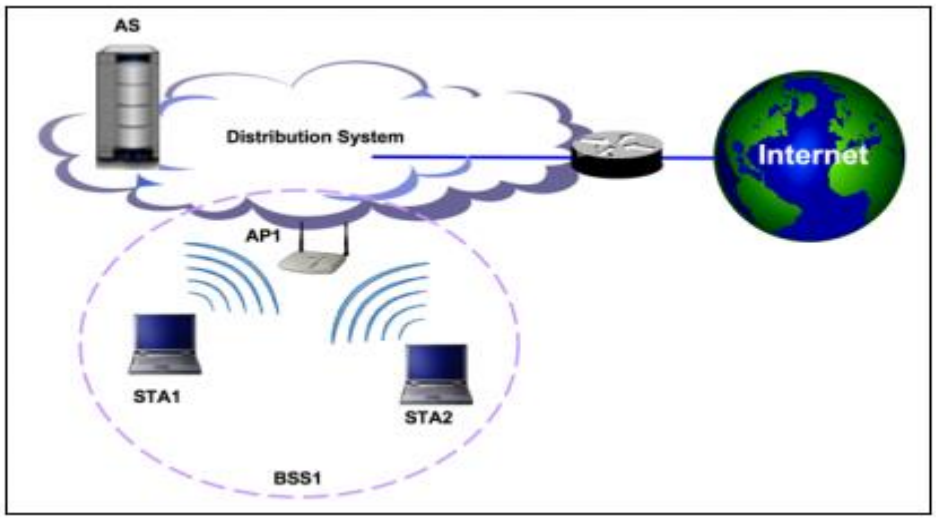

Figure: Conceptual View of Authentication Server in a Network

Q.29 Write short note on the following: 1. Server Backup Procedures 2. Recovering From a Security Compromise 3. Security Testing Servers

Ans:

1. Server Backup Procedures

- There are three types of server backup are as follows:

  i. Full backups

  - Full backups include the OS, applications, and data stored on the server.
  - The advantage of a full backup is that it is easy to restore the entire server to the state (e.g., configuration, patch level, data) it was in when the backup was performed.
  - The disadvantage of full backups is that they take considerable time and resources to perform.

  ii. Incremental backups

  - Incremental backups reduce the impact of backups by backing up only data that has changed since the previous backup.

  iii. Differential backups

  - Differential backups reduce the number of backup sets that must be accessed to restore a configuration by backing up all changed data since the last full backup.

- However, each differential backup increases as time lapses from the last full backup, requiring more processing time and storage than would an incremental backup.

2. Recovering From a Security Compromise

- Most organizations eventually face a successful compromise of one or more hosts on their network.
- Organizations should create and document the required policies and procedures for responding to successful intrusions.
- Most organizations already have a dedicated incident response team in place, which should be contacted immediately when there is suspicion or confirmation of a compromise.
- Organization may wish to ensure that some of its staff are knowledgeable in the fields of computer and network forensics.
- A server administrator should follow the organization's policies and procedures for incident handling.
- The incident response team should be contacted for guidance before the organization takes any action after a suspected or confirmed security compromise.

3. Security Testing Servers

- Periodic security testing of servers is critical.
- Without periodic testing, there is no assurance that current protective measures are working or that the security patch applied by the server administrator is functioning as advertised.
- Although a variety of security testing techniques exists.

  i. Vulnerability Scanning

  - Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts.
  - Vulnerability scanners can help identify out-of-date software versions, missing patches, or system upgrades.
  - Vulnerability scanners rely on periodic updating of the vulnerability database to recognize the latest vulnerabilities.

  ii. Penetration Testing

  - Penetration testing is to exercise system protections by using common tools and techniques developed by attackers.
  - This testing is highly recommended for complex or critical servers.

Q.30 what is penetration testing?

Ans:

- Penetration testing is “security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation”.
- Penetration testing is to exercise system protections by using common tools and techniques developed by attackers.
- This testing is highly recommended for complex or critical servers.
- Penetration testing can be an invaluable technique to any organization's information security program.
- However, it is a very labor-intensive activity and requires great expertise to minimize the risk to targeted systems.
- Penetration testing does offer the following benefits:
    - Tests the network using the same methodologies and tools employed by attackers.
    - Verifies whether vulnerabilities exist
    - Goes beyond surface vulnerabilities and demonstrates how these vulnerabilities can be exploited iteratively to gain greater access.
    - Provides the “realism” necessary to address security issues.
    - Allows for testing of procedures and susceptibility of the human element to social engineering.

Q.31 Write a note on Identification & Authentication Technologies.

Ans:

Q.32. List and explain the important implementation issues for I&A systems.

Ans:

Q.33 what are various criteria used by the system to determine if a request for access will be granted?

Ans: