CHAPTER 1 – NETWORK SECURITY

1.1 IMPLEMENT SECURITY CONFIGURATION PARAMETERS ON NETWORK DEVICES AND OTHER TECHNOLOGIES.

Firewalls

Firewall configuration, administration and operational procedures should be documented. Configuration of multiple firewalls should be identical. Integrity checks of the configuration files of the firewall should be performed regularly.

Routers

A router relays packets across multiple networks by using a special routing table based upon network addresses. It may be configured to stop broadcast traffic, but is generally slower than a bridge due to the extra processing involved.

Switches

Switches, like hubs, provide network connectivity amongst groups of nodes. Switches have supplanted hubs in today's networks. This is primarily due to the fact that hubs split up the total throughput available amongst connected nodes, whereas switches provide full advertised throughputs speeds to all connected nodes. Intelligent switches can also perform basic routing and bridging functions.

Load Balancers

To achieve scalability, more servers can be added to the network configuration so as to distribute the load amongst them. This workload distribution mechanism is known as load balancing. With multiple servers in a server group, network traffic can be evenly distributed among these servers.

Proxies

A proxy server can be either software or hardware based. It intercepts messages entering and leaving the network and makes outgoing requests on behalf of internal nodes. It is used primarily to mask the IP addresses of nodes connected to the Internet.

Web security gateways

An application gateway applies security mechanisms to specific applications. A Web Security Gateway defends against advanced attacks via real time threat analysis capability. Use of these two kinds of gateways in conjunction with packet filtering routers can offer a higher level of security.
VPN concentrators

VPN concentrators are hardware based devices. They usually come with advanced encryption and authentication techniques capable of implementing remote-access or site-to-site VPNs.

NIDS and NIPS

An IDS can be hardware or software based. It inspects inbound and outbound network activity and identifies suspicious patterns that may be a sign of attack. It can also analyze the information it gathers and compare it to the available attack signatures. IPS is the next step up as it carries out proactive actions against the detected threats. Each type of IPS works differently, depending on the way they “think”. Specifically these include Behavior based, Signature based, Anomaly based, and Heuristic.

A knowledge-based IDS is signature and references a database of previous attack profiles/signatures. This technique produces lower overall false alarm rates than its behavior-based counterpart. Its main drawback is the database must be continually updated. A behavior-based system is statistical anomaly–based and works by referencing a baseline for identifying intrusion attempts. It is more dynamic but can produce higher false alarm rates. Heuristic IDS is also anomaly based. It uses a model of acceptable behavior. Exceptions to that model are flagged for alert. Heuristic intrusion detection activities are often classified into good/benign, suspicious, and unknown.

Protocol analyzers

Protocol analyzers are used to capture and log unicast, multicast and broadcast traffic passing through a network. This requires a network adapter that can run in promiscuous mode. They are also sometimes referred to as packet sniffer.

Spam filter

In order to protect against email spamming, spam filter software should be installed. Spam filters may work at the server side or at the client end, depending on the software chosen. In order to facilitate this more completely, unused mail daemons should be removed and suspicious activities should be detected and recorded.

All-in-one security appliances

(URL filter, Content inspection, Malware inspection)

All-in-one appliances are hardware devices. They offer security functions that are tightly integrated with networking functions such as routing, wireless access, etc. Most of these devices include features such as URL filter, Content inspection, and Malware inspection.

Web application firewall vs. network firewall

A web application firewall is an appliance with the primary duty of applying rules to HTTP conversations to protect against application attacks. A network firewall is different. It is a network layer firewall that runs at a low level of the TCP/IP stack to filter packets.
Application aware devices
(Firewalls, IPS, IDS, Proxies)

Application aware devices have systems in place which are capable of maintaining information about connected applications to optimize their operation. Many of the modern firewalls, IPS, IDS and proxies are application aware devices.

1.2 PLAN AND IMPLEMENT A SERVER DEPLOYMENT INFRASTRUCTURE

Rule-based management

Rule-based management involves having security decisions made in real time via scripted policy rules. Rules can be used to replace or complement the more traditional role based management.

Firewall rules

A firewall prevents unauthorized access to or from a private network by examining each message and/or packet that passes through it. It examines each packet entering or leaving the network and accepts or drops it based on the pre-defined firewall rules. Rule based firewalls in general deploy more sophisticated mechanisms than simple packet filtering.

VLAN management

A VLAN is a group of computers on multiple LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on different LANs. VLAN capable switches or routers allow for this kind of logical connection. There are usually separate management ports for performing VLAN management.

Typically all VLANs are configured on a trunked link. ISL and 802.1Q are the VLAN trunking protocols used with Fast Ethernet, while the VLAN trunking protocol is for FDDI.

Secure router configuration

Routing takes place at Layer 3. A security breach at this layer can be catastrophic. Therefore, the necessary security measures as recommended by the router vendor to secure the router should be implemented. Additionally, make sure all the latest OS patches and firmware updates are applied.

Access control lists

A fundamental way of enforcing privilege separation and controlling access is the use of access control lists (ACLs). Under this system, an ACCESS_MASK is specific to an object being created. When an attempt is made to open the object, the username will be verified against the discretionary access control list obtained from the security descriptor.
Port Security

A switch can be flooded with invalid source MAC addresses until the switch’s CAM table is full. Port security is a measure that can be deployed against such attack. It is recommended to limit the number of MAC addresses available on a switch port.

802.1x

802.1x is an IEEE standard that provides Port-based Network Access Control (PNAC). It makes use of the physical access characteristics of the existing LAN infrastructure to perform authentication and authorization of devices attached to the LAN.

Flood guards

Denial of service (DoS) attacks are designed to render the target unusable. Flooding is overloading the capabilities of a machine or network. Distributed denial of service (DDoS) uses a large number of compromised hosts to flood a target system with network requests. A flood guard system or software can be used to defend against such flooding attempts.

Loop protection

Loop protection in a network often involves the use of the Spanning-Tree Protocol (STP). STP prevents bridging loops in an Ethernet network by setting one and only one switch as a root bridge and blocking the other redundant data paths. Rootguard and BPDUGuard can be configured on the switch port to secure the STP operation.

Implicit deny

"Everything not explicitly permitted is forbidden" is the basic definition of default or implicit deny. This is based upon the principle of least privilege.

Network separation

Segmenting via network separation can provide users additional bandwidth without upgrading all equipment. Separating LANs breaks a network into smaller pieces so that routers can be used to block network broadcast or other malicious attempts.

Log analysis

Packet sniffer is used to intercept and log network traffic that passes through a network. Unicast, multicast and broadcast traffic and should be captured and logged. Subsequent performance of log analysis differentiates and defines the captured traffic, creating a picture of the overall network security.

Unified Threat Management

Unified threat management (UTM) is a comprehensive solution that is all-inclusive. This means it can perform multiple security functions via one appliance.
1.3 Plan and Implement Server Upgrade and Migration

**DMZ**

A demilitarized zone (DMZ) is a small IP subnetwork that sits between the trusted internal LAN and the public Internet. It is considered an extra layer of protection for those hosts running behind the firewall.

**Subnetting**

A network can be segmented with a switch or a router. Basic switches have all hosts on the same IP subnet. With a router, hosts attached to the router ports are not necessarily on the same subnet. The final design of the subnets depends on the level of segmentation and traffic isolation needed or desired.

**VLAN**

VLANs are beneficial since the use of broadcast domains can eliminate the need for routing equipment to handle unnecessary broadcast traffic. In fact, a VLAN can accommodate smaller groups of users who need to communicate among themselves and no one else. To implement a VLAN, the switch must be VLAN capable.

VLAN filtering can be carried out through a Layer 2 port or a Layer 3 port after routing. VLAN ACLs are used to filter traffic between VLAN devices.

**NAT**

Some firewall and proxy software perform Network Address Translation (NAT). This allows a LAN to use a set of IP addresses for internal traffic and another set for external traffic. This is useful when there are many internal clients but limited IP addresses.

**Remote Access**

Remote access allows users to a network from outside via a normal phone or Internet connection. Once a connection is made the user can access any programs or data on the network subject to security clearance via the remote access server.

**Telephony**

IP Telephony (IPT) describes how circuit switched voice signals can be converted to the format of data packets. Analog voice signal has to be digitized into pulse code modulation (PCM) signals via a voice coder-decoder. The PCM samples have to be compressed for transmission.

**NAC**

The term Network Access Control (NAC) refers to the emerging approach of unifying different endpoint security technologies, authentication and security enforcement. Some vendors refer to NAC as Network Admission Control.
Virtualization

By implementing virtualization, a physical device may act like there are multiple physical versions of itself. This allows scalable sharing across the entire network. Note that virtualization often relies on the help of multiple processor cores that sit within the same processor die.

Cloud Computing
(Platform as a Service, Software as a Service, Infrastructure as a Service, Private, Public, Hybrid, Community)

Cloud computing is a form of distributed computing. With it, an application is built using resources from multiple services from the different locations. When the endpoint to access the services is known, software can be used as a service, much like utility computing. There are many variations to cloud computing, including Platform as a Service, Software as a Service, Infrastructure as a Service, Private, Public, Hybrid, and Community.

Layered security / Defense in depth

Defense in depth means more than one subsystem has to be breached to compromise the security of the system and the stored information. A typical defense in depth approach calls for dividing the various security elements into layers, which is why it is considered a layered security approach.

1.4 GIVEN A SCENARIO, IMPLEMENT COMMON PROTOCOLS AND SERVICES.

Protocols

A protocol is the language that both hosts must follow in order to communicate. Computers generally send and receive data as packets. A protocol works at the various levels of the OSI model to disassemble, and reassemble packets. Some of these protocols include IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS HTTPSC, SCP, ICMP, IPv4, IPv6, Iscsi, Fibre Channel, FCoE, FTP SFTP, TFTP, TELNET, HTTP, and NetBIOS.

Ports

A port is an electronic number that a given protocol uses to communicate. These numbers can vary depending on which transmission protocol is at use. For example, FTP, Telnet, and SMTP use TCP while TFTP and SNMP use UDP. FTP uses port #21. Telnet uses port #23. SMTP uses port #25. SNMP uses port #161. FTP / TFTP are used for file transfer. Telnet is used for terminal emulation. SNMP is used to monitor and manage a network.

NetBEUI implements the NetBIOS Frame transport protocol for use by the small Windows based local network. Novell's IPX/SPX is the protocol stack supported by Netware. Appletalk is used by Apple clients.

OSI relevance

The OSI model is a network reference model that has 7 layers. IP runs at layer 3, while TCP runs at layer 4. Each OSI layer communicates with the corresponding layer on the receiving end.
1.5 **Given a scenario, troubleshoot security issues related to wireless networking.**

**WPA**

WiFi Protected Access (WPA) provides payload integrity but it does not use Advanced Encryption Standard (AES). It is still considered to be more secure than WEP.

**WPA2**

WPA 2 creates fresh new session keys on every association. Due to this, the encryption keys used for each client are unique and client specific.

**WEP**

Wired Equivalent Privacy (WEP) is an older standard that uses cyclic redundancy check (CRC). It is less secure when dealing with payload integrity.

**EAP**

Extensible Authentication Protocol (EAP) offers the capability to deploy RADIUS in an Ethernet network.

**PEAP**

Protected EAP (PEAP) is a version of EAP jointly developed by RSA, MS and Cisco. It relies on server-side PKI to create an encrypted EAP-TLS tunnel.

**LEAP**

LEAP is Cisco’s version of EAP. It uses TKIP and dynamic WEP keys. It has since been replaced by PEAP.

**MAC filter**

MAC filtering can be used to examine the hardware address of wireless clients that are allowed to connect to the AP. Every wireless adaptor has a MAC address hard coded into it.

**Disable SSID broadcast**

SSID broadcasts should be enabled to make it difficult for attackers to learn the SSID of wireless devices. The SSID should be difficult to guess.

**TKIP**

Temporal Key Integrity Protocol (TKIP) dynamically generates security keys. It is the primary reason that WPA is a more robust form of wireless security.
CCMP

Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an AES-based encryption mode used by WPA2 for providing strong security. It uses a 128-bit key.

Antenna Placement

The manner in which electromagnetic waves move is determined partially by polarization. Vertical polarization means the wave moves up and down, while horizontal polarization means the wave moves left and right. Circular means the wave circles when moving forward. Hertz antennas are usually installed above ground to radiate vertically or horizontally. Marconi antennas have one end grounded and are installed perpendicular to the ground surface.

Power level controls

Power level controls limit the decibel output of the wireless devices to control their range of broadcast. Signal gain is stated as a ratio of input to output power, and may be expressed in decibels (dB). Decibels express power, gain or loss, in logarithmic form and also against a reference.

Captive portals

A captive portal is a type of web page commonly found on public-access networks. This kind of web page requires the user to view and interact (such as agreeing to terms of use) before giving access to the public network.

Antenna types

A dipole antenna has two identical conductive elements bilaterally symmetrical. A monopole antenna has one conductor with one side of the feedline connected. An omnidirectional antenna propagates signals 360-degrees.

Site surveys

A site survey has the goal of determining the number and placement of APs for providing adequate coverage. It is required for any wireless network installation and implementation effort.

VPN (over open wireless)

When making a VPN connection over an unsecured wireless network, it is possible for an attacker to hijack the connection. To add more security to the VPN connection, certificates can be used to perform verification/validation for the connections.