Security+ Cram Notes

2. Technologies and Tools

2.1 Install and configure network components, both hardware and software-based, to support organizational security

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. A VPN provides a mechanism to access corporate networks safely using Internet. VPN uses encryption to ensure only authorized user can access the corporate resources. A secure tunnel is created through the public network through which the packets are transported between the remote computer and the corporate network. VPN are used for accessing a corporate network securely from remote locations using public Internet.

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

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

1. Gateway-to-gateway VPN
2. Gateway-to-host VPN
3. Host-to-gateway VPN
4. 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.

There are two widely known protocols that can be implemented for enabling VPN communications:

1. PPTP
2. L2TP

PPTP stands for Point to Point Tunneling Protocol. It is a PPTP is pioneered by Microsoft and others is a widely used protocol.

L2TP stands for Layer Two (2) Tunneling Protocol. L2TP merges the best features of PPTP and

L2F (from Cisco Systems).

PPTP and L2TP protocols together with PPP protocol enable ISPs to operate Virtual Private Networks (VPNs).

Ipsec: The two primary security services that are provided by IPSec are:

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

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

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.

HSM:A hardware security module (HSM) is a hardware encryption device that's connected to a server, typically using PCI, SCSI, serial, or USB interfaces and managed separately from the operating system. These modules provide a secure hardware store for CA keys, as well as a dedicated cryptographic processor to accelerate signing and encrypting operations.

DMZ:Demilitarized zone (DMZ) A network segment that exists in a semi-protected zone between the Internet and the inner, secure trusted network.
Jump Server: A jump host (also known as a jump server) is an intermediary host or an SSH gateway to a remote network, through which a connection can be made to another host in a dissimilar security zone, for example a demilitarized zone (DMZ). It bridges two dissimilar security zones and offers controlled access between them.

HTML5: HTML5 is the current version of the HTML protocol standard, and this version was developed to handle the modern web content of audio and video as well as to enhance the ability of a browser to function without add-ins such as Flash, Java, and browser helper objects for common functions.

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.

Flood guard: Flood guard is a defence mechanism against flooding type of attacks such as distributed Denial of Service (DDoS) attacks. Floodguards are used to prevent massive attacks against a public or private network.

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.

Firewall:

- The Packet Filters work at Network Layer of OSI model.
- The Application Layer Proxy works at the Application Layer of OSI model
- A Firewall implemented with stateful technology (like Checkpoint Firewall) works at all layers of the OSI model.
- 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.

NAT: 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. It 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.

ACL(Access Control List): An ACL specifies which users or system processes are granted

access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject, an operator, and an object. For instance, if a file has an ACL that contains (Alex, delete, file-name), this would give Alex permission to delete the file. ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface. ACL statements are processed top-down until a match is found, and then no more statements in the list are processed. If no match is found in the ACL, the packet is dropped due to implicit deny. That is, you down type specifically to drop the traffic, but it is understood by the ACL to drop all traffic that does not match atleast one of the statements.

NIDS: As opposed to Network Intrusion Detection Systems (NIDS), Network Intrusion Prevention Systems (NIPS) focus on prevention. Arguably, NIPS is a subset of NIDS. Honeyspot is an example of NIPS

Vampire tape: A vampire tap is a type of connection that hooks directly into a coax by piercing the outer sheath and making contact with the center conductor. A vampire tap is widely used in 10Base5 networks. The mechanism allows an attacker to monitor network traffic without being detected.

Network Access Control (NAC): NAC controls access to a network with policies, including pre-admission checks and security policy checks and post-admission controls as and when a user or a device connects to a network and determines what they can do. Other schemes such as NAT, private addressing, and subnetting are only security mechanisms that take care of only one aspect of network security, and not policy based as in case of NAC.

Data loss prevention (DLP): DLP may used for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer. DLP solution can be used to filter documents sent to a printer based on the content, thus disabling any sensitive data from being transmitted to the printer.

USB Blocking: Microsoft Windows 7 comes with bit locker technology to encrypt files. You can use the same to encrypt USB drive. Note that the motherboard also should support encryption for bit-locker technology to work. If you use file-level encryption, you need to encrypt the required file separately. That may again pose problem as you may forget to encrypt or forget the key used for file-level encryption. Further, some encryption programs does not support file-level encryption.

MAC Filtering: MAC filtering is a security access control method in which MAC address is used to determine access to the network. With MAC Filtering each host is identified by its MAC address and allowed (or denied) access based on that

SSL decryptor: Another layer of security can be added to the network with an SSL decryptor . These gateways decrypt encrypted traffic (SSL or TLS), inspect it, and then re-encrypt it before sending it on to its destination. It is a processor-intensive process, but the advantage it offers is in the inspection step-making sure that you are not forwarding problems that did not get caught simply because the data was encrypted.

Port spanning/port mirroring

Access Point (TAP): TAP is a passive signal-copying mechanism installed between two points on the network. The TAP can copy all packets it receives, rebuilding a copy of all messages. TAPs provide the one distinct advantage of not being overwhelmed by traffic levels, at least not in the process of data collection. Port taps, when placed between sending and receiving devices,can be used to carry out man-in-the-middle attacks. Thus, when placed by an unauthorized party, they can be a security risk.

An aggregator switches is a device that takes multiple inputs and combines them to a single output.

Port Spanning/Port Mirroring: Most enterprise switches have the ability to copy the activity of one or more ports through a Switch Port Analyzer (SPAN) port, also known as a port mirror. This traffic can then be sent to a device for analysis. Port mirrors can have issues when traffic levels get heavy, as the aggregate SPAN traffic can exceed the throughput of the device.

Mitigation techniques

Runbooks: Operations runbooks, often simply called runbooks, are a set of standardized documents, references, and procedures used to describe common IT tasks. Runbooks are created for the purpose of walking someone through the steps necessary for accomplishing a specific task or troubleshooting a particular issue

Playbooks: A playbook is a set of approved steps and actions required to successfully respond to a specific incident or threat. Playbooks are commonly instantiated as itemized checklists, with all pertinent data prefilled in systems, team members, actions, and so on.

Firewall rules: Firewall rules state whether the firewall should allow particular traffic to pass through or block it. The structure of a firewall rule can range from simple to very complex,depending on the type of firewall and the type of traffic.

Mobile Device Management (MDM): MDM is the term for a collective set of commonly employed protection elements associated with mobile devices.

Quarantine: In the case of a suspicious file, file change,or configuration change, there is a chance of error in the decision, and having a virtual "undo" capability may be desired. This is where the concept of quarantine enters the equation. Quarantining an item is to render it disabled but not permanently removed from the system.

Installing and configuring wireless security settings involves securing the wireless network from unauthorized access and protecting sensitive data from being intercepted. The following are steps to consider when securing a wireless network:

1**. Choose a secure wireless encryption protocol:** The most common encryption protocols are WEP, WPA, and WPA2. WPA2 is the most secure, but WPA is also a strong option.

2. Change the default SSID: The Service Set Identifier (SSID) is the name of the wireless network. It's important to change the default SSID to prevent hackers from finding the network.

3. Enable MAC filtering: MAC filtering allows only authorized devices to connect to the network by verifying the device's MAC address.

4. Disable WPS: WPS (Wi-Fi Protected Setup) is a feature that makes it easy to set up a wireless network, but it can also make it easier for hackers to gain access.

5. Enable WPA2-Enterprise with 802.1X: This is a more secure option that requires user authentication and encryption.

6. Use a strong password: The password for the wireless network should be strong, including a mix of letters, numbers, and symbols.

7. Disable broadcast of the SSID: Disabling the broadcast of the SSID makes it more difficult for unauthorized users to find the network.

8. Disable remote management: Unless it's necessary, it's best to disable remote management of the wireless router to prevent unauthorized access.

9. Keep the firmware up-to-date: Updating the firmware of the wireless router helps to protect against known vulnerabilities.

By following these steps, you can help to secure your wireless network and protect sensitive data.

Installing and configuring authentication protocols

1. Extensible Authentication Protocol (EAP): EAP is a flexible authentication protocol used in wireless networks and point-to-point connections. It allows the use of multiple authentication methods such as certificates, one-time passwords, and biometrics. To configure EAP, you need to set up an authentication server such as RADIUS server and configure the wireless access point to use EAP and connect to the RADIUS server for authentication.

2. Protected Extensible Authentication Protocol (PEAP): PEAP is a variation of EAP that provides an encrypted tunnel for the authentication process. It uses SSL or TLS to secure the communication between the client and the authentication server. To configure PEAP, you need to set up an authentication server such as RADIUS server with a certificate, configure the wireless access point to use PEAP, and configure the client devices to use PEAP with the appropriate certificate.

3. EAP-FAST: EAP-FAST is a proprietary EAP type developed by Cisco Systems. It provides a secure and scalable authentication solution for wireless networks. To configure EAP-FAST, you need to set up an authentication server, configure the wireless access point to use EAP-FAST, and configure the client devices to use EAP-FAST with the appropriate certificate.

4. EAP-TLS: EAP-TLS is an EAP type that uses certificates for authentication. It provides a secure and scalable solution for wireless networks and is often used in enterprise environments. To configure EAP-TLS, you need to set up a RADIUS server with a certificate, configure the wireless access point to use EAP-TLS, and configure the client devices to use EAP-TLS with the appropriate certificate.

5. EAP-TTLS: EAP-TTLS is a variation of EAP that provides a secure and scalable solution for wireless networks. It uses SSL or TLS to secure the communication between the client and the authentication server. To configure EAP-TTLS, you need to set up a RADIUS server with a certificate, configure the wireless access point to use EAP-TTLS, and configure the client devices to use EAP-TTLS with the appropriate certificate.

6. IEEE 802.1X: 802.1X is a network port-based authentication protocol used in wired and wireless networks. It provides a secure and scalable solution for network access control. To configure 802.1X, you need to set up an authentication server, configure the network switch or wireless access point to use 802.1X, and configure the client devices to use 802.1X with the appropriate certificate or credentials.

7. Remote Authentication Dial-in User Service (RADIUS) Federation: RADIUS is a protocol used for remote authentication and authorization. RADIUS federation allows multiple RADIUS servers to be used for authentication in a single network. To configure RADIUS federation, you need to set up multiple RADIUS servers, configure each RADIUS server to

trust the others, and configure the network devices to use RADIUS federation for authentication.

Note: The exact steps to install and configure these protocols may vary depending on your specific network setup and device. It is always recommended to consult the documentation of the specific device or operating system you are using.

Note that EAP and other protocols can work with various authentication servers, including RADIUS, LDAP, and Kerberos. The specific authentication server used with EAP /PEAP/ 802.1X etc. depends on the requirements of the network and the available infrastructure. RADIUS is a commonly used authentication server for wireless networks, and EAP-RADIUS is one of the most widely deployed authentication methods for wireless networks. However, it's important to note that EAP is a framework and can work with different authentication servers, not just RADIUS.

Methods
The methods for installing and configuring wireless security settings include:

Pre-shared key (PSK): This method uses a shared secret key that is agreed upon by the wireless access point (AP) and the wireless client. The secret key is used to encrypt and decrypt wireless traffic, providing a basic level of security. There are two types of PSK: personal (for home use) and enterprise (for business use). The personal PSK is easier to set up, but less secure than the enterprise PSK, which requires a RADIUS server to authenticate clients.

WiFi Protected Setup (WPS): This is a simple method of setting up a secure wireless network without the need to manually configure encryption keys. It uses a combination of push-button and PIN methods to securely connect a client device to the AP.

Captive portals: This method is commonly used in public places like coffee shops, hotels, and airports. A captive portal is a web page that is displayed when a client device connects to a wireless network. The user must authenticate or accept terms and conditions before they can access the internet.

In summary, EAP works with any authentication server, not just RADIUS. However, the authentication server that is used in conjunction with EAP may vary depending on the method used to set up wireless security.

Installation considerations

-Site surveys
-Heat maps

-WiFi analyzers
-Channel overlaps
-Wireless access point (WAP) placement
-Controller and access point security

When installing wireless security settings, there are several important considerations to keep in mind. One of the first steps is to conduct a site survey, which helps you understand the physical layout of your environment and how the wireless signals will propagate. This information can be used to create heat maps that help you visualize the wireless signal coverage and strength.

Additionally, using WiFi analyzers can help you determine the optimal channels to use and help you identify any channel overlaps that may cause interference. Placement of wireless access points is also important as they should be placed in a way that ensures maximum coverage while avoiding dead spots.

Another important consideration is the security of the wireless network. This includes securing both the wireless access points and the wireless network controllers. Implementing strong authentication methods and encryption protocols, such as WPA2-AES, is essential to prevent unauthorized access to the network. Also, using captive portals to control access to the network and limit the risk of malicious actors exploiting vulnerabilities in the network.

Access point configuration

Example1: Set SSID on the generic WAP router to SECNET.

Configuration steps:

Network Name (SSID) is basically the device's wireless network name and is one way of securing your wireless network. The SSID is shared by all devices in your wireless network and therefore, has to be unique since this will identify your wireless network from the rest.

To change the wireless network name of your router, follow the steps below.

Note: SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSIDs.

1. In Access point window click **"Wireless"** tab

2. In that look for "Wireless Network Name" (SSID), and enter the SSID name "SECNET" in

the box provided. Click on **"Save & Exit"** button.

***Note**: The exercise is typical for a particular brand of home router and may differ slightly from device to device. When you are configuring any other brand/make routers, please read the manufacturer's documentation provided along with the device.*

Example2: Using the simulator, perform the task of disabling SSID broadcast.

A **Service Set Identifier (SSID)** is the **wireless network name** broadcast by the wireless device such as a wireless router. When another wireless device searches the area for wireless networks it will detect the SSID to be able to associate with the router. SSID Broadcast is enabled by default however; you may also choose to disable it.

Disabling the **SSID Broadcast** is one way of securing your wireless network. This procedure will prevent other users from detecting your SSID or your wireless network name when they attempt to view the available wireless networks in your area.

To disable the SSID Broadcast of your Linksys router, follow these steps:

1. In Access point window click **"Wireless"** tab

2. Click **"Disable"** radio button against **"Wireless SSID Broadcast"** and click **"Save & Exit"** button.