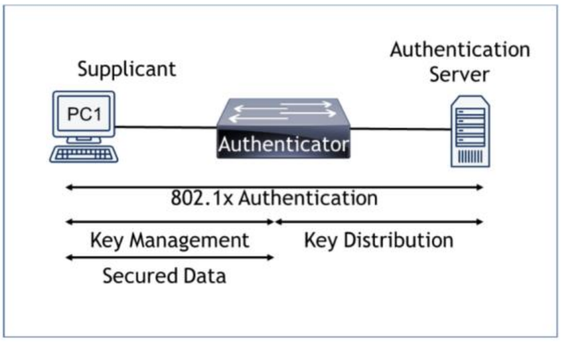
Sec+ 501 Get Certified Topic 4 – Securing Your Networking

CH 4 – EXPLORING ADVANCED SECURITY DEVICES

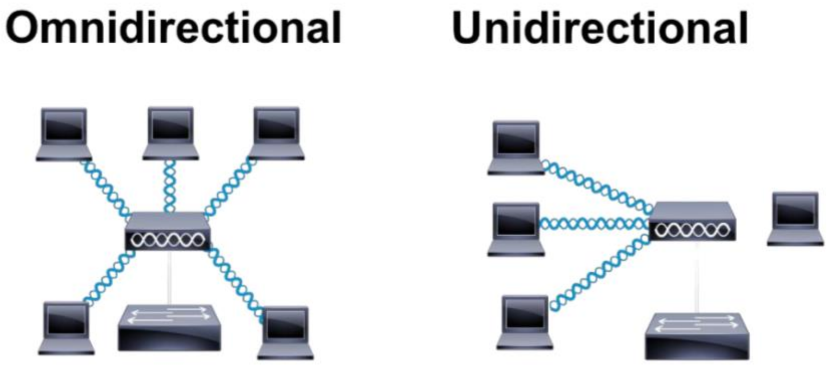
- HIDS – Host based Intrusion Detection System
  - Monitors all traffic on a single host system such as a server or workstation.
  - Can detect malicious activity missed by antivirus software.
- NIDS – Network based Intrusion Detection System
  - Installed on network devices/sensors such as routers or firewalls to monitor network traffic and detect network based attacks
  - May not be able to detect anomalies on individual systems/workstations unless there is an anomaly in the network traffic.
  - Can also use taps or port mirrors to capture traffic.
  - Cannot monitor encrypted traffic and cannot monitor traffic on individual hosts
- Syn Flood Attack – common DoS attack. Instead of a three way handshake from Syn → ←SYN/ACK→ACK, attacker sends multiple SYN packets but never completes third part of TCP handshake with last ACK packet.
  - Like pulling out your hand from a handshake.
  - Consumes resources on server and may crash server, preventing users from connecting
- **Remember this:**
  - **Signature-based detection identifies issues based on known attacks or vulnerabilities. Signature-based detection systems can detect known anomalies.**
  - **Anomaly-based detection can detect unknown anomalies. Start at a baseline then compare network traffic against baseline. If anything is uncommon, IDS sends alert**
  - **Policy based – Detection based on Policies (E.G: No Telnet Authorized)**
- True positive
  - Malicious activity is identified as an attack

- False positive
    - Legitimate activity is identified as an attack
- True negative
- • Legitimate activity is identified as legitimate traffic
- False negative
    - Malicious activity is identified as legitimate traffic
- IPS – Intrusion Prevention System
    - Can prevent attacks unlike IDS which can only log/detect
    - Placed inline with traffic (in-band)
    - IDS collects data passively (out-of-band)
- IPS is a preventive control.
- SSL/TLS accelerators – hardware devices focused on TLS traffic. Provides encryption. Best to place as close as possible to related devices.
- SSL Decryptor – Place in DMZ, and redirect all traffic to and from the Internet through it. Often used with NIPS. Allows NIPS to inspect unencrypted traffic and prevent attacks. Malicious traffic can get through if its encrypted.
- SDN – Software Defined Network
    - Uses Virtualisation technologies to route traffic instead of using hardware routers and switches.
    - Separates data planes and control planes within a network.
- Honeynet – Group of honeypots with a separate network or zone, but accessible from an organization’s primary network.
- Honeypot – Server intentionally left open
- **Remember this:**
    - **Honeypots and honeynets attempt to divert attackers from live networks. They give security personnel an opportunity to observe current methodologies used in attacks and gather intelligence on these attacks.**
- IEE 802.1x – Port based authentication protocol
    - Ensures only authorized clients can connect to a network.
    - Prevents rogue devices from connecting
    - Possible to combine with a VLAN and RADIUS



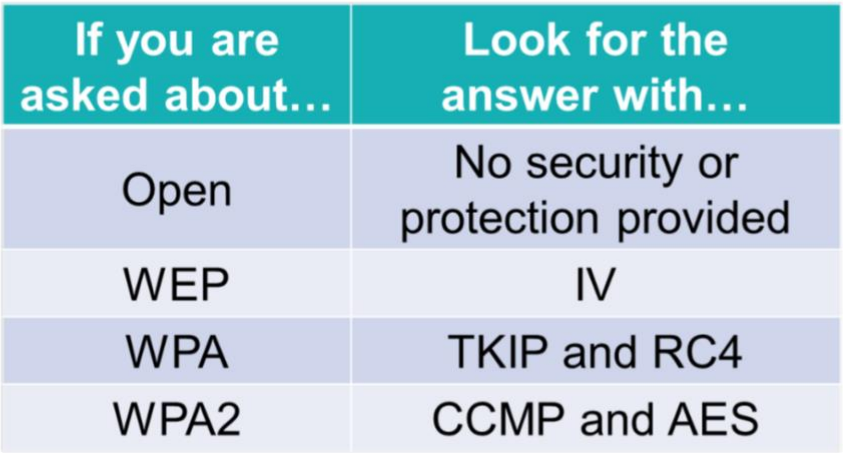
- AP – Access point
- WAP – Wireless Access Point
  - Connects wireless clients to a wired network. Also have routing capabilities.
  - All wireless routers are AP's
  - Not all AP's are routers.
  - Most AP include physical ports
- Fat AP – Stand alone, intelligent, autonomous AP including everything needed to connect wireless clients to a wireless network
  - Includes Routing components, NAT, DHCP, ACLs, wireless security options etc.
- Thin AP – controller based AP
  - Is not a stand-alone AP. AP managed by a controller. Admins use wireless controller to configure/manage this AP.
- **Remember this:**
  - **Fat AP is also known as a stand-alone AP and is managed independently. Thin AP is also known as a controller based AP and is managed by a wireless controller. Wireless controller configures thin AP.**
- Wireless B (22MHz), G(20MHz), and N use a 2.4 GHz signal (20MHZ and 40 MHz)
- Wireless A,N, and AC use a 5.0 GHz signal (20,40,80,160 MHz)
- 2.4GHz signals can travel further than 5GHz
  - Bigger Freq means shorter wavelength being used, signal travels shorter distance
- SSID – Service Set Identifier
  - Identifies name of wireless network. You should change SSID from default name.

    - Disabling SSID broadcast can hide the network from casual users, but an attacker can easily discover it with a wireless sniffer
- **Remember this:**
    - **MAC filtering can restrict access to a wireless network to specific clients however an attacker can use a sniffer to discover allowed MAC addresses and circumvent this form of network access control. It's relatively simple for an attacker to spoof a MAC address.**
- **Remember this:**
    - **You can limit the range of an AP to a room or building by reducing the AP's power level. This prevents people from connecting as they will be out of AP's range.**
- Antennas:



    - Omnidirectional Antenna
        - Access point radios out signal equally in each direction. Can be Dangerous.
    - Unidirectional Antenna
        - Transmission power focuses on a single direction. Allows you to choose which areas receive signals
- AD HOC mode – Wireless devices connect to each other without an AP.
- WEP – Wired Equivalent Privacy
    - Original 802.11 wireless security standard that claims to be as secure as a wired network
    - WEP's weakness is its 24-bit IV (Initialization Vector)
- WPA – WiFi Protected Access

  - Replacement for WEP. Susceptible to password-cracking attacks through wireless protocol analyser then offline brute force attack. Can use disassociation attack
- WPA2 – Stronger version of WPA.
- TKIP – Temporal Key Integrity Protocol
  - Older Encryption protocol used with WPA.
- CCMP – Counter Mode Cipher Block Chaining
  - Encryption Protocol used by WPA2



If you are asked about…	Look for the answer with…
Open	No security or protection provided
WEP	IV
WPA	TKIP and RC4
WPA2	CCMP and AES

- **Remember this: PSK(preshared key) mode (WPA-PSK or WPA2-PSK) uses a preshared key and does not provide individual authentication. Open mode doesn't use any security and allows all users to access AP. Enterprise mode is more secure than personal mode, and provides strong authentication. Enterprise uses an 8021.x server (implemented as a RADIUS server) to add authentication.**
- Enterprise – Forces users to authenticate with unique credentials before granting them access to wireless network. When you select Enterprise mode you need to enter 3 pieces of information:
  - RADIUS Server (AAAA server)- Enter IP addressed assigned to 802.1x server
  - RADIUS port – Enter port used by RADIUS server. Usually 1812, but may also be 1645.
  - Shared Secret

AUTHENTICATION PROTOCOLS

- EAP –
  - Extensible Authentication Protocol(EAP)

    - A framework of protocols that allows for numerous methods of authentication including passwords, digital certificates, and public key infrastructure
    - EAP-MD5 uses simple passwords for its challenge-authentication
    - EAP-TLS uses digital certificates for mutual authentication. Extension of PEAP.
    - EAP-TTLS uses a server-side digital certificate and a client-side password for mutual authentication
    - EAP-FAST
        - Provides flexible authentication via secure tunneling (FAST) by using a protected access credential instead of a certificate for mutual authentication
    - Protected EAP(PEAP)
        - Supports mutual authentication by using server certificates and Microsoft's Active Directory to authenticate a client's password. Extra layer of protection for EAP. Encrypts EAP with TLS.
    - Radius Federation
- **Remember this:**
    - **Enterprise mode requires an 802.1x server. EAP – FAST supports certificates. PEAP and EAP – TTLS require a certificate on the 802.1x server. EAP-TLS also use TLS, but require certificates on both 802.1x server and each of the clients**
- Captive Portal – Solution that forces clients using web browsers to complete a specific process before it allows them to access that network.
    - Free Internet Access
        - Hospitals, restaurants
    - Paid Internet Access
        - Resorts, Hotels, Cruise ships, Airlines
    - Alternative to IEEE 802.1x – Captive portal is an alternative as adding a 802.1x server may be expensive

ATTACKS

- Disassociation Attack
  - Effectively removes a wireless client form a wireless network, forcing it to reauthenticate. WPS allow users to easily configure a wireless device by entering an 8 digit PIN. A WPA attack guesses all possible PINS until it finds correct one. Will usually discover PIN within hours and use it to discover passphrase.
  - Attack that targets an individual client connected to a network, forces it offline by deauthenticating it, and then captures the handshake when it reconnects
- WPS (WiFi-Protected Setup)
  - Allows users to configure wireless devices without typing passphrase.
  - Automated encryption setup for wireless networks at a push of a button, but is severely flawed and vulnerable.
  - Susceptible to brute force
  - Always disable WPS
- Rogue AP – Rogue Access Point
  - AP placed within network without official authorization.
  - An unauthorized WAP or Wireless Router that allows access to the secure network
- Evil Twin – Rogue Access point with same SSID as a legitimate access point.
  - E.G: Attacker sets up AP using same SSID as the public Wi-Fi network of a coffee shop and unsuspecting users will connect to the evil twin instead.
- **Remember this:**
  - **Rogues access points are often used to capture and exfiltrate data. An evil twin is a rogue access point using same SSID as a legitimate access point. A secure AP blocks unauthorized users, but a rogue access point provides access to unauthorized users.**
- Jamming Attack
  - Intentional radio frequency interference targeting your wireless network to cause a denial of service condition

  - Wireless site survey software and spectrum analyzers can help identify jamming and interference
- IV attacks
  - Attempts to discover pre shared key from IV. Used in WEP.
- NFC Attacks – Near field communication
  - NFC - Allows two devices to transmit information when they are within close range through automated pairing and transmission
  - NFC devices are operated within 4 cm from each other
  - NFC attack – Attacker uses NFC reader to capture data from another NFC device. Can be used through eavesdropping. NFC may use antenna to boost range.
- Bluejacking
  - Sending of unsolicited messages to Bluetooth-enabled devices such as mobile phones and tablets
- Bluesnarfing
  - Unauthorized access of information from a wireless device through a Bluetooth connection
- Replay attack –
  - Attacker captures data sent between two entities, modifies it and attempts to impersonate one of the parties by replaying the data.
  - WPA2 is not vulnerable to these attacks but WPA are. Check Table.
- Radio Frequency Identification(RFID)
  - Devices that use a radio frequency signal to transmit identifying information about the device or token holder
  - RFID can operate from 10 cm to 200 meters depending on the device
  - Include RFID reader and tags
- RFID Attack –
  - Used to track and mange inventory and any type of valuable assets including objects and animal.
  - Sniffing/Eavesdropping
  - Replay
  - DoS

- Misconfigured AP can also lead to wireless attacks
- VPN – Virtual Private Network
  - Allows end users to create a tunnel over an untrusted network and connect remotely and securely back into the enterprise network
  - Client-to-Site VPN or Remote Access VPN
  - VPN can be placed in a DMZ to reach through a public IP address.
- **Remember this:**
  - **VPN provides remote access to a private network via a public network. VPN concentrators are dedicated devices used for VPNS. Include all the services needed to create a secure VPN supporting many clients.**
- TLS may be used in some tunnelling protocols to secure VPN channel. E.G: SSTP through port 443.
- Split Tunnel – VPN admin determines what traffic should use in the encrypted tunnel
  - A remote worker’s machine diverts internal traffic over the VPN but external traffic over their own internet connection
  - Prevent split tunnelling through proper configuration and network segmentation
- Full Tunnel – All Traffic goes through VPN tunnel when user is connected to VPN
- IPSEC - A TCP/IP protocol that authenticates and encrypts IP packets and effectively securing communications between computers and devices
  - provides confidentiality (encryption), integrity (hashing), and authentication (key exchange)
  - Authentication through AH (Authentication Header)
  - Encryption through ESP (Encapsulating Security Payload) to encrypt data. ESP also includes AH and uses port 50.
- **Remember this: IPsec is a secure encryption protocol used with VPNs. Encapsulating Security Payload (ESP) provides confidentiality, integrity, and authentication for VPN traffic. IPsec uses Tunnel mode for VPN traffic and can be identified with protocol ID 50 for ESP. It uses IKE over port 500. A full tunnel**

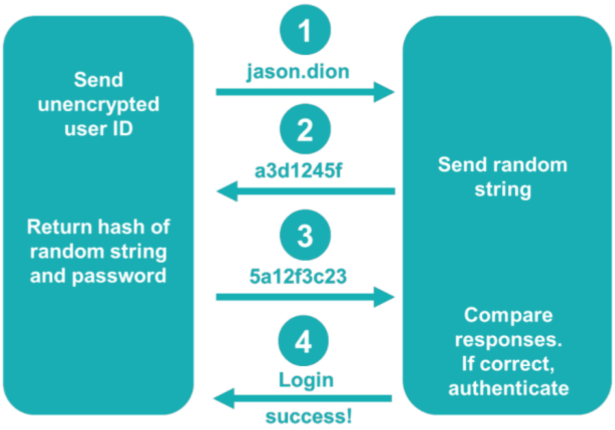
encrypts all traffic after a user has connected to a VPN. Split tunnel only encrypts traffic destined for the VPN's private network.

- Site to Site VPN – 2 VPN servers acting as gateways for 2 networks separated geographically.
  - E.G: HQ and remote office. 2 VPN servers act as gateways to connect networks at the 2 locations together.
- Always on VPN – VPN always on.
- NAC – Network Access Control
  - Security technique in which devices are scanned to determine its current state prior to being allowed access onto a given network
  - If a device fails the inspection, it is placed into digital quarantine
  - Persistent/Permanent Agents
  - A piece of software that is installed on the device requesting access to the network
  - Non-Persistent/Dissolvable Agents
  - Uses a piece of software that scans the device remotely or is installed and subsequently removed after the scan
- **Remember This:**
  - **NAC includes methods to inspect clients for health, such as having up to date antivirus software. NAC can restrict access of unhealthy clients to a remediation network. You can use NAC for VPN clients and for internal clients. Permanent agents are installed on the clients. Dissolvable agents (sometimes called agentless) are not installed on the clients and are often used to inspect employee-owned mobile devices.**

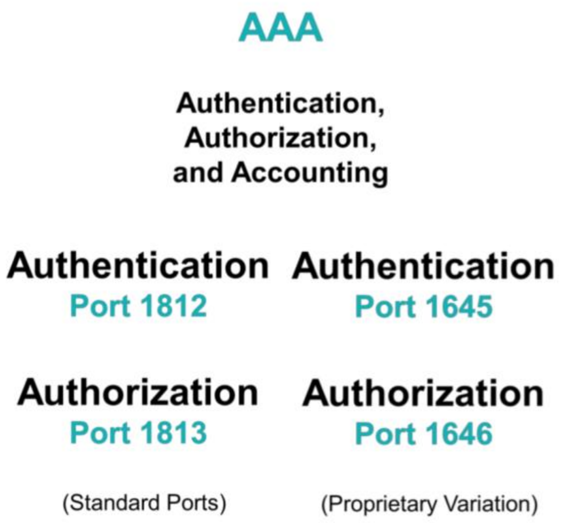
IDENTITY AND ACCESS SERVICES

- Password Authentication Protocol(PAP)
  - Used to provide authentication but is not considered secure since it transmits the login credentials/passwords unencrypted (in the clear) with cleartext
- Challenge Handshake Authentication Protocol(CHAP)

  - Used to provide authentication by using the user's password to encrypt a challenge string of random numbers. Uses a handshake process where server challenges client. Client then responds with appropriate authentication information.



- Microsoft's version of CHAP is MS-CHAP. MSCHAPv2 is improved version. Client authenticates the server
- PAP and CHAP used mostly with dial-up
- **Remember this:**
  - **PAP authentication uses a password or a PIN. A significant weakness is that PAP sends information across network in cleartext, making it susceptible to sniffing attacks. CHAP is more secure than PAP as passwords aren't sent over network in clear text.**
- RADIUS – Remote Authentication Dial – In User Service
  - Provides a centralized method of authentication for multiple remote access servers. RADIUS encrypts the password packets, but not entire authentication process.
  - Provides centralized administration of dial-up, VPN, and wireless authentication services for 802.1x and the Extensible Authentication Protocol (EAP)
  - RADIUS operates at the application layer
- TACACS+ - Terminal Access Controller Access-Control System
  - Alternative to ADIUS but proprietary to CISCO systems.
  - Benefit: Can interact with Kerberos.
  - Encrypts entire authentication process where RADIUS encrypts only password

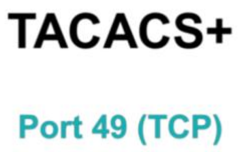


AAA

Authentication,
Authorization,
and Accounting

Authentication Port 1812	Authentication Port 1645
Authorization Port 1813	Authorization Port 1646
(Standard Ports)	(Proprietary Variation)

Cisco’s TACACS+ is a proprietary version of RADIUS



TACACS+

Port 49 (TCP)

- Diameter – Created to overcome some of the limitations of RADIUS and is often used instead of RADIUS.
- **Remember this:**
  - **RADIUS, TACAS+, and Diameter all provide centralized authentication. TACACS+ is proprietary to Cisco, but can be used with Kerberos. Diameter is an improvement over RADIUS and supports many additional capabilities, including securing transmissions with EAP. They are all AAA (Authentication, authorization, accounting) protocols as they provide all three services.**