Guía de Estudio en Español

CompTIA Security+ (SY0-701) — Capítulo 4

Securing Your Network — Asegurando tu Red

Este material es un **resumen conceptual elaborado con palabras propias**, pensado como guía de apoyo para estudiar junto al libro original en inglés. No es una traducción ni una reproducción del texto original; cubre los mismos temas, en el mismo orden, para facilitar el repaso en español.

Incluye: resumen por secciones, tablas comparativas, glosario EN↔ES y preguntas de práctica originales.

1. Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)

Ambos analizan tráfico para detectar posibles ataques, igual que un analizador de protocolos. La diferencia clave está en la **respuesta**: un IDS solo detecta y alerta; un IPS detecta y además previene el ataque activamente.

Característica	IDS	IPS
Ubicación	Fuera de banda (out-of-band), pasivo — usa un tap o puerto espejo.	En línea con el tráfico (in-line), activo — todo el tráfico pasa por él.
Capacidad	Detecta y alerta.	Detecta, reacciona y previene antes de que el ataque llegue.

1.1 HIDS vs. NIDS

- **HIDS (basado en host):** software instalado en un equipo específico (workstation o servidor). Monitorea el tráfico que llega por su NIC y también archivos críticos del sistema operativo. Puede detectar malware que el antivirus tradicional no detecta.
- **NIDS (basado en red):** usa sensores instalados en switches, routers o firewalls que reportan a una consola central. No puede detectar anomalías en un host individual (salvo que afecten el tráfico de red) ni analizar tráfico cifrado. Se puede usar un 'port mirror' o tap para copiar el tráfico de un switch hacia el sensor.

Ubicación de sensores: un sensor del lado de Internet ve todos los ataques (incluso los que el firewall bloquea); un sensor del lado interno solo ve lo que logró pasar el firewall.

1.2 Métodos de detección

- **Basado en firmas (signature-based):** compara el tráfico contra una base de datos de ataques y vulnerabilidades conocidas (similar al antivirus). Requiere actualizar la base regularmente.
- **Basado en tendencias / anomalías (trend-based):** primero establece una línea base (baseline) de comportamiento normal, y luego alerta cuando el tráfico se desvía significativamente. Es efectivo para detectar exploits de día cero (zero-day), ya que estos no tienen firma conocida.

1.3 Falsos positivos y falsos negativos

	Hay ataque real	No hay ataque
El sistema alerta	Verdadero positivo (correcto)	Falso positivo
El sistema no alerta	Falso negativo	Verdadero negativo (correcto)

El umbral (threshold) de alerta se ajusta buscando un equilibrio: demasiado bajo genera muchos falsos positivos (sobrecarga a los administradores); demasiado alto deja pasar ataques reales sin ser detectados (falsos negativos).

2. Tecnologías de Engaño (Honeypots y Similares)

- **Honeypot:** servidor señuelo que parece un objetivo fácil, diseñado para desviar al atacante de la red real y permitir observar sus métodos. Nunca contiene datos valiosos reales.
- **Honeynet:** conjunto de honeypots que imitan una red completa, muchas veces implementados como servidores virtuales dentro de un único servidor físico.
- **Honeyfile:** archivo señuelo con un nombre atractivo (ej. 'contraseñas.txt') diseñado para atraer la atención de un atacante.
- **Honeytoken:** un registro falso pero identificable insertado en una base de datos de producción, usado para detectar si los datos fueron robados (si ese registro aparece en otro lado, se confirma el robo).

3. Seguridad de Redes Inalámbricas

3.1 Conceptos básicos

Un **punto de acceso (AP)** conecta clientes inalámbricos a una red cableada. Un *router inalámbrico* es un AP con capacidad adicional de enrutamiento. Las redes Wi-Fi usan principalmente las bandas de **2.4 GHz** (mayor alcance) y **5 GHz** (mayor ancho de banda), divididas en canales que pueden solaparse entre sí, afectando el rendimiento.

- **SSID:** el nombre de la red inalámbrica. Se recomienda cambiar el SSID por defecto para no revelar el modelo del AP.
- **Filtrado MAC:** permite o bloquea dispositivos según su dirección MAC. Es fácil de burlar: un atacante puede detectar MACs autorizadas con un sniffer y clonarlas (*MAC cloning/spoofing*).
- **Site survey y heat maps:** el 'site survey' examina el entorno inalámbrico (interferencias, cobertura). Un *heat map* muestra con colores la intensidad de la señal en distintas zonas. El 'wireless footprinting' combina esto con un plano del edificio para ubicar APs y zonas muertas.
- **Antenas:** las omnidireccionales transmiten en todas direcciones; las direccionales concentran la señal en una sola dirección, logrando mayor alcance.

3.2 Protocolos criptográficos inalámbricos

WEP y WPA están obsoletos y no deben usarse. Los protocolos vigentes son:

Protocolo	Cifrado	Modos
WPA2	AES con CCMP	Abierto, PSK (clave precompartida) o Enterprise.
WPA3	AES con mejoras	Abierto mejorado (cifra incluso sin autenticación), SAE (reemplaza PSK) o Enterprise.

- **Modo abierto:** sin seguridad, datos en texto plano.
- **Modo PSK:** acceso anónimo con una frase/clave compartida — da autorización pero no autenticación individual (no hay usuario, solo una clave compartida).
- **Modo Enterprise:** exige autenticación individual mediante un servidor 802.1X (típicamente RADIUS), con usuario y contraseña únicos (o certificados).
- **SAE (WPA3):** reemplaza el PSK de WPA2 con defensas criptográficas más fuertes.

3.3 Protocolos de autenticación (EAP)

Muchos servidores 802.1X usan variantes del Extensible Authentication Protocol (EAP). La diferencia clave entre ellas es si requieren certificados digitales:

Método	Certificado en servidor	Certificado en cliente
PEAP	Sí	No
EAP-TTLS	Sí	No

EAP-TLS	Sí	Sí (el más seguro)
EAP-FAST	No (usa PAC en su lugar)	No

802.1X: protocolo de autenticación basado en puerto — exige que un dispositivo se autentique antes de acceder a un puerto físico o a un AP, evitando que dispositivos no autorizados (rogue) se conecten.

Captive portal: obliga al usuario a completar un proceso (aceptar términos, pagar, iniciar sesión) antes de otorgar acceso a Internet. Es común en hoteles, hospitales y como alternativa más económica a un servidor 802.1X.

4. Ataques Inalámbricos

Ataque	Descripción
Disociación (disassociation)	Envía una trama de desconexión falsificando la MAC de la víctima, forzándola a reautenticarse.
WPS	Fuerza bruta contra el PIN de 8 dígitos de Wi-Fi Protected Setup para luego obtener la contraseña de la red (vulnerable en WPA2, mitigado en WPA3).
Rogue AP	Punto de acceso no autorizado conectado a la red (por un empleado o un atacante), usado para capturar o exfiltrar tráfico.
Evil twin	Rogue AP que usa el mismo SSID (o muy similar) que uno legítimo, para engañar a los usuarios y capturar sus credenciales.
Jamming	Denegación de servicio: inunda la frecuencia con ruido para interferir la señal legítima.
Ataque de IV	Explota la reutilización del vector de inicialización (IV) para descubrir la clave precompartida — vulnerabilidad clásica de WEP.
NFC	Un lector NFC con antena potenciada intercepta datos de una transacción cercana (ej. pago sin contacto).
RFID	Incluye sniffing/espionaje, clonación de etiquetas (RFID cloning) y DoS por interferencia.
Bluejacking	Envío de mensajes no solicitados a un dispositivo Bluetooth cercano (mayormente inofensivo).
Bluesnarfing	Acceso o robo no autorizado de información de un dispositivo Bluetooth (contactos, correos, etc.).
Bluebugging	Como bluesnarfing, pero instala una puerta trasera con control total del teléfono (llamadas, mensajes).

War driving / war flying: práctica de recorrer una zona (en auto, a pie, en avión o con drones) buscando redes inalámbricas vulnerables; también se usa como auditoría defensiva para detectar rogue APs y evil twins. Colocar dispositivos en una jaula de Faraday bloquea los ataques Bluetooth.

5. VPN para Acceso Remoto

Una VPN da acceso a una red privada a través de una red pública (generalmente Internet), cifrando el tráfico dentro de un túnel. Se puede implementar en un servidor con NICs dedicadas, o con un **concentrador VPN** dedicado (más común en organizaciones grandes), típicamente ubicado en la subred filtrada (DMZ).

5.1 Protocolos de túnel

- **IPsec:** el más usado con VPNs. Modo *Túnel* cifra todo el paquete IP (encabezados incluidos) — oculta las IP internas y es el modo típico de una VPN. Modo *Transporte* solo cifra el contenido (payload), usado dentro de redes privadas, no en VPNs. Usa **AH** (Authentication Header, protocolo IP 51) para autenticación e integridad, y **ESP** (Encapsulating Security Payload, protocolo IP 50) para cifrado, autenticación e integridad. Usa IKE sobre el puerto 500 para establecer el canal seguro.
- **TLS/SSTP:** cifra el túnel VPN sobre el puerto 443 — útil cuando IPsec no es viable (ej. detrás de NAT).
- **L2TP:** protocolo de túnel sin cifrado propio; se combina con IPsec para cifrar los datos.
- **Portal VPN HTML5:** permite conectarse vía navegador usando TLS, útil para dar acceso puntual a pocos usuarios (ej. un consultor externo).

5.2 Túnel completo vs. túnel dividido

En un **túnel dividido (split tunnel)**, solo el tráfico destinado a la red privada pasa por el túnel cifrado; el resto (ej. una búsqueda en Internet) sale directo por el ISP del usuario. En un **túnel completo (full tunnel)**, todo el tráfico del usuario pasa por el túnel cifrado, permitiendo aplicar filtros de contenido corporativos (UTM) pero siendo más lento.

5.3 Modelos de VPN

- **Acceso remoto (host-to-gateway):** el usuario se conecta directamente al servidor VPN; es consciente del proceso.
- **Sitio a sitio (site-to-site):** dos gateways VPN conectan dos redes geográficas distintas de forma transparente para los usuarios.
- **Always-on VPN:** se conecta automáticamente en cuanto el dispositivo tiene Internet, usado tanto en site-to-site como en acceso directo (ej. celulares).

6. Control de Acceso a la Red (NAC)

El NAC inspecciona la 'salud' de un dispositivo (antivirus actualizado, parches al día, firewall activo) antes de darle acceso completo a la red. Si el equipo no cumple las condiciones, se lo redirige a una **red de remediación / cuarentena** con los recursos necesarios para ponerse al día.

- **Agente permanente:** se instala en el cliente y queda ahí de forma indefinida.
- **Agente disolvente (dissolvable):** se descarga y ejecuta al conectarse, y se elimina después de reportar el estado (a veces llamado 'sin agente', aunque igual usa uno temporalmente).
- **Sin agente (agentless) real:** escanea el cliente de forma remota sin instalar ningún código en él.

El NAC puede aplicarse tanto a clientes VPN como a clientes internos (ej. visitantes que conectan un cable en una sala de reuniones).

7. Protocolos de Autenticación Remota y AAA

Protocolo	Característica clave
PAP	Envía la contraseña en texto plano — inseguro, solo como último recurso.
CHAP	Más seguro que PAP; usa un proceso de saludo (handshake) con hash y un valor único (nonce), sin enviar la contraseña en claro.
RADIUS	Autenticación centralizada; usa UDP; por defecto cifra solo la contraseña (puede combinarse con EAP para cifrar toda la sesión).
TACACS+	Alternativa de Cisco a RADIUS; usa TCP; cifra toda la sesión por defecto; usa múltiples desafíos y respuestas; puede integrarse con Kerberos.

AAA: RADIUS, TACACS+ y Diameter son protocolos AAA completos (autenticación, autorización y auditoría/accounting). Kerberos a veces se menciona como protocolo AAA, pero no ofrece auditoría por sí mismo, aunque puede integrarse con sistemas que sí la brindan.

8. Glosario de Términos Clave (Inglés ↔ Español)

Inglés	Español	Definición breve
IDS / IPS	IDS / IPS	Sistema de detección / prevención de intrusiones.
HIDS / NIDS	HIDS / NIDS	IDS basado en host / basado en red.
Signature-based / trend-based	Basado en firmas / en tendencias	Métodos de detección de un IDS/IPS.
Baseline	Línea base	Comportamiento normal usado como referencia para detectar anomalías.
False positive / negative	Falso positivo / negativo	Alerta sin ataque real / ausencia de alerta ante un ataque real.
In-line / out-of-band	En línea / fuera de banda	El tráfico pasa por el dispositivo, o no.
Honeypot / honeynet	Honeypot / honeynet	Señuelo(s) para desviar y observar atacantes.
Honeytoken	Honeytoken	Registro falso para detectar robo de datos.
SSID	SSID	Nombre de la red inalámbrica.
MAC filtering	Filtrado MAC	Restringe acceso según dirección MAC (fácil de burlar).
Site survey / heat map	Estudio de sitio / mapa de calor	Análisis de cobertura y calidad de señal inalámbrica.
WPA2 / WPA3	WPA2 / WPA3	Protocolos criptográficos vigentes para Wi-Fi.
PSK / SAE	PSK / SAE	Clave precompartida (WPA2) / su reemplazo más seguro (WPA3).
802.1X	802.1X	Autenticación basada en puerto.
EAP / PEAP / EAP-TLS	EAP / PEAP / EAP-TLS	Familia de protocolos de autenticación extensible.
Captive portal	Portal cautivo	Fuerza un proceso antes de dar acceso a la red.
Rogue AP / Evil twin	AP fraudulento / gemelo malvado	AP no autorizado / AP con SSID falsificado.

Inglés	Español	Definición breve
Jamming	Interferencia (jamming)	DoS que inunda la frecuencia con ruido.
Bluesnarfing / bluebugging	Bluesnarfing / bluebugging	Robo de datos / control total vía Bluetooth.
VPN concentrator	Concentrador VPN	Dispositivo dedicado que centraliza conexiones VPN.
Split tunnel / full tunnel	Túnel dividido / completo	Solo tráfico privado cifrado / todo el tráfico cifrado.
IPsec (AH / ESP)	IPsec (AH / ESP)	Protocolo de cifrado IP; autenticación / cifrado del túnel.
NAC	Control de acceso a la red	Verifica la 'salud' de un dispositivo antes de darle acceso.
Quarantine / remediation network	Red de cuarentena / remediación	Red aislada para equipos que no cumplen los requisitos de salud.
RADIUS / TACACS+	RADIUS / TACACS+	Protocolos de autenticación centralizada (AAA).

9. Preguntas de Práctica (Autoevaluación)

Preguntas de elaboración propia, en español, para repasar los conceptos del capítulo 4. Las respuestas están al final.

1. Un sistema detecta un ataque comparando el tráfico contra una base de datos de patrones conocidos. ¿Qué método de detección está usando?

2. Un dispositivo de seguridad está ubicado en línea con el tráfico y puede bloquear paquetes maliciosos antes de que lleguen a la red interna. ¿Es un IDS o un IPS?

3. Una empresa coloca un archivo llamado 'contraseñas_admin.txt' con credenciales falsas en el escritorio de varios servidores para atraer a posibles atacantes internos. ¿Cómo se llama esta técnica?

4. Un usuario se conecta a una red Wi-Fi pública sin necesidad de usuario ni contraseña, solo aceptando términos de uso en una página que aparece automáticamente. ¿Cómo se llama esta página?

5. Un atacante configura un punto de acceso con el mismo SSID que el Wi-Fi gratuito de un aeropuerto para capturar credenciales de los usuarios que se conectan por error. ¿Qué tipo de ataque es?

6. Una organización exige que los usuarios se autentiquen individualmente con usuario y contraseña antes de acceder a la red Wi-Fi corporativa, usando un servidor RADIUS. ¿Qué modo de WPA2/WPA3 están usando?

7. Un protocolo de autenticación remota exige certificados digitales tanto en el servidor como en cada cliente. ¿Cuál es, de los métodos EAP vistos?

8. Una VPN está configurada para que solo el tráfico dirigido a la red privada de la empresa pase por el túnel cifrado, mientras que la navegación normal del usuario sale directo a Internet. ¿Qué tipo de túnel es?

9. Un sistema verifica que el antivirus y los parches de un dispositivo estén actualizados antes de permitirle acceso completo a la red, y si no cumple, lo redirige a una red aislada. ¿Cómo se llama este sistema?

10. Una empresa quiere que las credenciales completas (no solo la contraseña) viajen cifradas por defecto al autenticar el acceso a los routers y switches de la red. ¿RADIUS o TACACS+ sería la mejor opción?

Respuestas

1. Detección basada en firmas (signature-based) — compara contra patrones de ataques conocidos.

2. Es un IPS — está en línea con el tráfico y puede prevenir el ataque, no solo detectarlo.

3. Un honeyfile — un archivo señuelo diseñado para atraer la atención de un atacante.

4. Un portal cautivo (captive portal).

5. Un evil twin (gemelo malvado) — un AP fraudulento con el mismo SSID que uno legítimo.

6. Modo Enterprise — usa un servidor 802.1X (RADIUS) para autenticación individual.

7. EAP-TLS — es el único que exige certificados en ambos extremos, servidor y cliente.

8. Túnel dividido (split tunnel) — solo el tráfico hacia la red privada pasa por el túnel cifrado.

9. Control de acceso a la red (NAC) — verifica la 'salud' del dispositivo antes de otorgar acceso completo.

10. TACACS+ — cifra toda la sesión de autenticación por defecto, mientras que RADIUS solo cifra la contraseña por defecto.
