Nombre : Jose Ismael Font Fernandez

Curso : Técnico en ciberseguridad

Facilitador Kelvin Feliz

Modulo : CCNA1

La gestión del **Inventario de Redes** es un proceso que va más allá de un simple listado de hardware; es una disciplina estratégica dentro de la **Gestión del Ciclo de Vida de Activos de TI (ITAM)**. El inventario se convierte en la única fuente de verdad para la seguridad, el cumplimiento normativo, la planificación financiera y la eficiencia operativa.

5. Profundización en la Gestión del Ciclo de Vida (ITAM)

El inventario es un componente de la disciplina ITAM, que divide la vida útil de un activo en fases bien definidas. Mantener el inventario actualizado en cada fase es crucial.

A. Fases del Ciclo de Vida del Activo

Fase ITAM	Descripción y Tareas del Inventario	Implicación en la Red
1. Planificación y Adquisición	Se define la necesidad y se aprueba la compra. El inventario se utiliza para revisar si existen **activos subutilizados** que puedan ser reasignados.	Se reservan los nombres de *host* y las **Direcciones IP** en el sistema IPAM antes de que el equipo llegue físicamente.
2. Despliegue (Commissioning)	El activo se instala, se configura y se pone en producción. Es el momento de **captura inicial de datos** (Modelo, Nº de Serie, Versión de *Firmware*, Ubicación exacta, Puertos de *Switch* conectados).	Se verifica que el activo cumpla con la **configuración base de seguridad** y se integra al sistema de monitoreo (SNMP).
3. Operación y Mantenimiento	Fase más larga. El inventario registra todos los **cambios de configuración**, parches de seguridad (nivel de *patching*), **asignación de**	Se actualiza continuamente la **CMDB** para reflejar las relaciones de dependencia (qué servicios soporta).

	usuario y el estado de la garantía.	
4. Retiro (Decommissioning)	El activo llega al final de su vida útil (**EoL/EoS**). El inventario documenta la baja, asegurando que se liberen recursos lógicos y se elimine toda la información sensible.	Se borra la **Dirección IP** del sistema IPAM, se desactiva el puerto del *switch* y se eliminan las entradas DNS para evitar conflictos futuros.

B. Mantenimiento de la Precisión

La precisión es el mayor desafío. Para garantizarla, se utilizan:

- **Conciliación Automática:** Herramientas que comparan datos de múltiples fuentes (SNMP, DHCP, agentes de *endpoint*) y resaltan discrepancias para que el administrador pueda corregirlas.
- **Historización:** Mantener un registro de los cambios (quién lo hizo, cuándo y por qué) para poder revertir configuraciones o rastrear la causa raíz de un fallo.

6. Seguridad y Cumplimiento Normativo

El inventario de red es la primera línea de defensa en una estrategia de ciberseguridad.

A. Fundamento de la Seguridad

1. **Gestión de Vulnerabilidades:** Un inventario preciso permite cruzar los modelos y versiones de *firmware* con bases de datos públicas de vulnerabilidades (CVE). Esto permite identificar rápidamente todos los equipos afectados por una nueva vulnerabilidad crítica y priorizar la aplicación de parches.
2. **Control de Acceso (NAC):** Las soluciones de **Network Access Control** dependen de un inventario preciso para verificar que solo los dispositivos conocidos y autorizados (comparando su MAC/IP) puedan acceder a la red.
3. **Detección de "Shadow IT":** El inventario continuo identifica activos no autorizados o desconocidos conectados a la red (*Shadow IT*), que representan un riesgo masivo para la seguridad.

B. Cumplimiento Regulatorio

Para marcos como GDPR, HIPAA o ISO 27001, las organizaciones deben demostrar control sobre los activos que almacenan o procesan datos sensibles.

- El inventario debe incluir campos específicos para marcar si un activo está **dentro del alcance** de una determinada regulación (ej: *Servidor que maneja información de tarjetas de crédito*).
- Se requiere documentar que los activos obsoletos han sido retirados siguiendo protocolos seguros de **destrucción de datos**.

7. Gestión Avanzada de Direcciones IP (IPAM)

La Gestión de Direcciones IP (IPAM) es la extensión lógica del inventario a la capa de red. Es la herramienta que organiza y automatiza el espacio de direccionamiento.

A. Funciones Centrales del IPAM

Función	Descripción Detallada	Beneficio
Monitoreo de Subredes	Supervisa el uso de cada subred, calculando direcciones usadas, disponibles, de red y de *broadcast* para IPv4. En IPv6, maneja el vasto espacio de direccionamiento jerárquico.	**Previene el agotamiento de direcciones** y facilita la planificación de capacidad.
Integración DDI	Cohesiona los tres servicios clave de la red: **D**NS (nombres), **D**HCP (asignación dinámica) e **I**PAM (documentación central).	Evita la entrada manual de datos en sistemas separados, **minimizando errores** y conflictos de IP.
Detección de Conflictos	Detecta cuando dos *hosts* intentan utilizar la misma dirección IP. Las herramientas IPAM avanzadas pueden incluso localizar el puerto exacto del *switch* donde está conectado el *host* malicioso.	**Asegura la estabilidad** de la red y el correcto funcionamiento del protocolo TCP.

B. Desafío IPv6

El espacio IPv6 es tan grande que el monitoreo manual es imposible. El IPAM es indispensable para:

- **Identificar Prefijos:** Gestionar la jerarquía de los prefijos de red de 48 bits, las subredes de 64 bits y los identificadores de interfaz.
- **Soporte a SLAAC:** Documentar las direcciones que los dispositivos se asignan a sí mismos automáticamente a través de la autoconfiguración sin estado (SLAAC).

8. Inventario en Arquitecturas Modernas

La virtualización y la nube han transformado la forma de realizar el inventario.

A. Inventario en Ambientes Virtuales

Los activos virtuales (Máquinas Virtuales, Contenedores, *Cloud Instances*) requieren herramientas que se integren directamente con el hipervisor (*VMware ESXi, Hyper-V*) o el orquestador (*Kubernetes*).

- El inventario debe registrar **atributos virtuales** como la cantidad de vCPUs, la RAM asignada dinámicamente, y la relación con el *host* físico subyacente.
- La baja volatilidad de estos activos obliga a que el descubrimiento sea continuo y en **tiempo real**, no periódico.

B. Desafío del Inventario Basado en la Nube (Cloud)

El inventario de activos en la nube pública (servidores en AWS, Azure) requiere un enfoque diferente, ya que no son directamente accesibles por SNMP o escaneo de red tradicional.

- Las herramientas de inventario deben utilizar las **APIs (Application Programming Interfaces)** de los proveedores de nube para consultar los metadatos de las instancias, los identificadores de recursos y la región geográfica donde están alojados los servicios.

En resumen, el Inventario de Redes ha evolucionado de un simple registro a una herramienta de **inteligencia de negocios y seguridad** que requiere automatización profunda y una visión centralizada a través de herramientas como la CMDB e IPAM, abarcando desde el cable físico hasta los servicios en la nube.

-