Ciberseguridad en Entornos de las Tecnologías de la Información

Módulo 5021 – Incidentes de Ciberseguridad

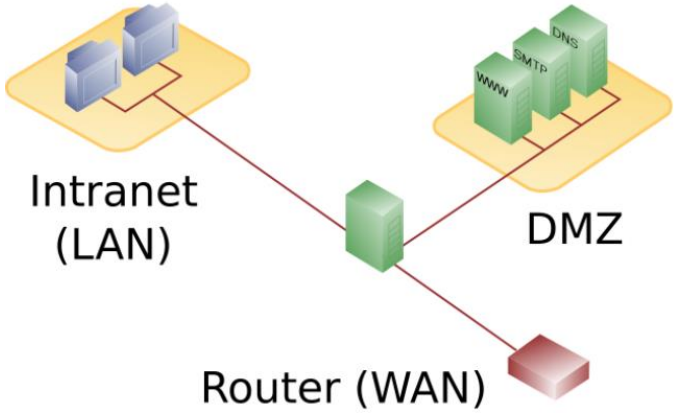
Ejercicio – Estructura en Trípode

Pliego de Descargo

- *Los ejercicios y conocimientos contenidos en el Módulo 5021, Incidentes de Ciberseguridad, tienen un propósito exclusivamente formativo, por lo que **nunca se deberán utilizar con fines maliciosos o delictivos.***
- *Ni el Ministerio de Educación y Formación Profesional como organismo oficial, ni el CIDEAD como área integrada en el mismo, serán responsables en ningún caso de los daños directos o indirectos que pudieran derivarse del uso inadecuado de las herramientas de hacking ético utilizadas en dichos ejercicios.*

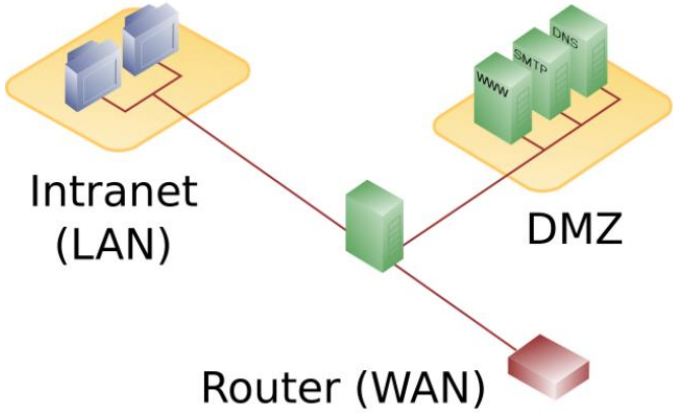
Implementación de una Estructura en Trípode con Zona Desmilitarizada

- Por lo general, cuando se utiliza una estructura en Trípode, desde la WAN sólo se puede acceder a una serie de máquinas preparadas para dar servicio hacia el exterior, que protegen la LAN de ataques. Estas máquinas constituyen lo que se denomina la Zona Desmilitarizada o DMZ.
- En esta estructura, sólo ciertas máquinas de la DMZ pueden acceder a la LAN en la que se sitúan los servidores con información sensible (por ejemplo, el inventario de activos o registro de planta), no permitiéndose nunca el acceso directo desde la WAN a la LAN.



El Vértice del Trípode

- El punto central en el que confluyen las tres patas del Trípode suele ser un Conmutador dotado de un Firewall, en el que se programan las reglas correspondientes para permitir sólo aquellos accesos que respeten los protocolos de seguridad de la empresa.
- En este ejemplo, se tratará de un conmutador profesional, asociado a un Firewall SW que estará incluido en la LAN.
- Para implementar esta estructura se establecerá el correspondiente Plan de Direcciones y las Reglas del Firewall para proteger la LAN de ataques externos.



Ejemplo de Estructura en Trípode con un SOC y un Inventario de Activos

INVENTARIO ACTIVOS SCI

RPi MySQL

FIREWALL

RPi Ubuntu UFW

DMZ

IDS – SIEM – NAS - VAULT

THREE-LEGGED SWITCH

3com 3300XM

INTERNET

OLT

CONEXIÓN INTERNET

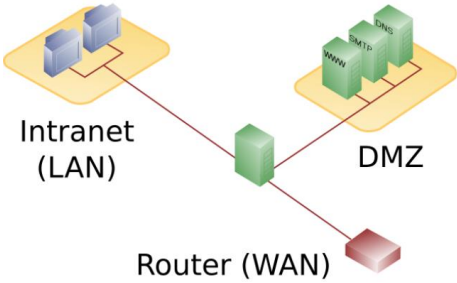
ONT/ROUTER

Ejemplo de Estructura en Trípode - DMZ, LAB y LAN

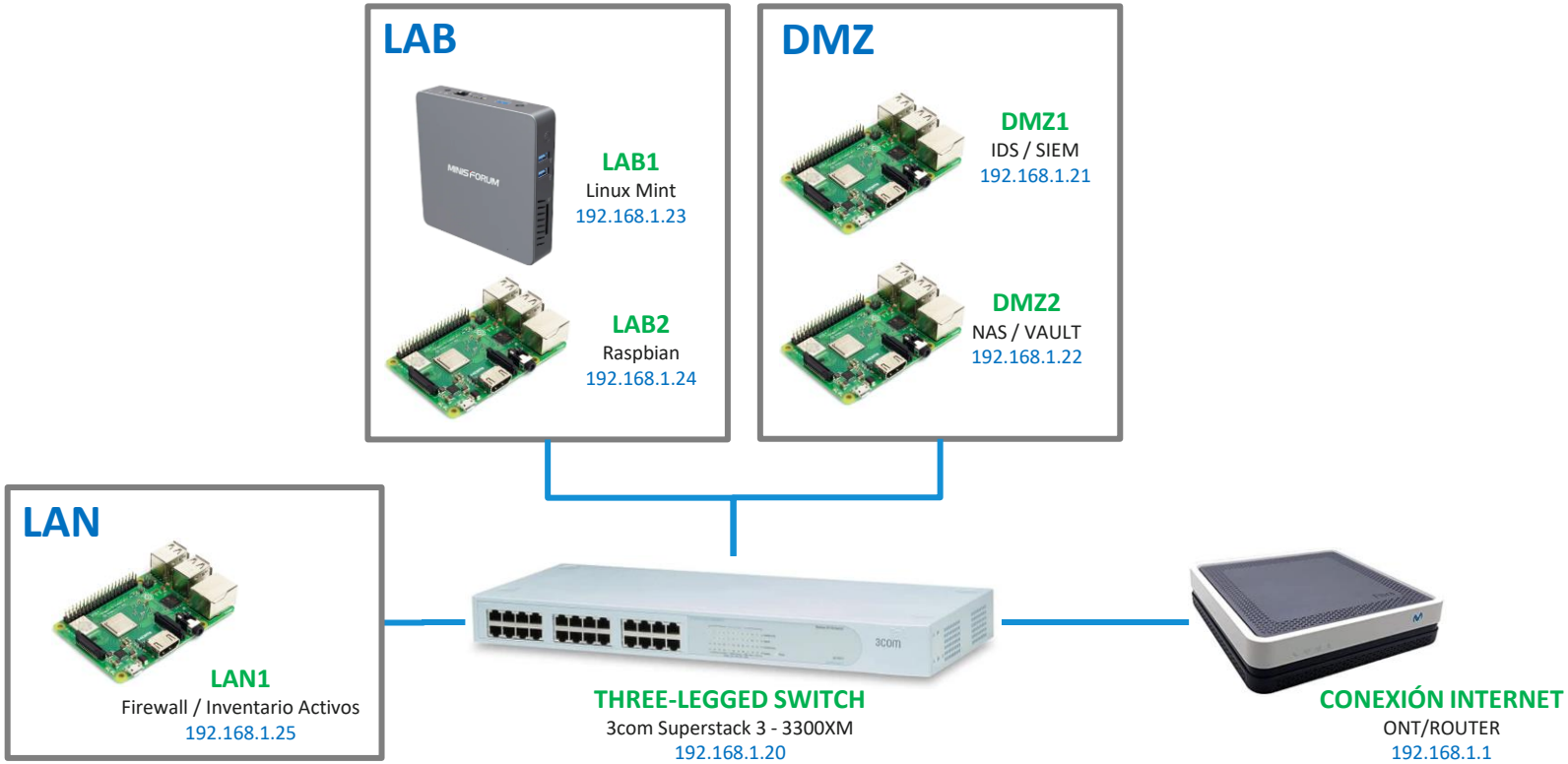
La estructura de red estará compuesta por las áreas siguientes:

- **Zona Desmilitarizada.** Estas máquinas constituirán el Front-End hacia la WAN.
- **Laboratorio.** Servidores de trabajo en los que se efectuarán las Pruebas de Sistemas.
- **Red de Área Local** o **Intranet.** Servidores con información sensible, como el Inventario de Activos.

Una vez determinadas las máquinas que se integrarán en cada área, se podrá diseñar la Topología de Red junto con el **Plan de Direcciones IP** asociado a la misma.



Ejemplo de Estructura en Trípode - Topología de Red



La Estructura en Trípode en el Inventario de Activos

Nombre Host	Dirección IP Estática	Sistema Operativo	Modelo Máquina	Función en el SOC	Observaciones
Router	192.168.1.1	Askey SO	RTF3505VW	Conexión Internet	LAN, WiFi
Switch	192.168.1.20	3com SO	SuperStack 3 3300XM	Three-Legged Switch	LAN, WiFi Inhabilitada
DMZ1	192.168.1.21	Raspbian	Raspberry Pi 4B	IDS / SIEM	LAN, WiFi Inhabilitada
DMZ2	192.168.1.22	Raspbian	Raspberry Pi 3B+	NAS / VAULT	LAN, WiFi Inhabilitada
LAB1	192.168.1.23	Linux Mint	MinisForum N34	Laboratorio Ubuntu / Debian	LAN, WiFi Inhabilitada
LAB2	192.168.1.24	Raspbian	Raspberry Pi 3B+	Laboratorio Raspbian	LAN, WiFi Inhabilitada
LAN1	192.168.1.25	Raspbian	Raspberry Pi 2B	Firewall / Inventario Activos	LAN, WiFi Inhabilitada

- La tabla anterior es una vista del Inventario de Activos en la que se pueden observar los datos de las máquinas que integran la Estructura en Trípode del ejemplo.