Actividad Evaluativa Taller

Tiempo de trabajo del estudiante: 20 horas

Habilidades de pensamiento a desarrollar:

Habilidades de orden básico	Observar	*x*	Identificar	*x*	Comparar	
	Relacionar	*x*	Ordenar		Clasificar jerárquicamente	
Habilidades de integración	Analizar	*x*	Sintetizar		Evaluar	
Habilidades de orden superior	Metacognición		Toma de decisiones		Pensamiento crítico	*x*
	Pensamiento creativo	*x*	Análisis de historia conceptual	*x*		

Nombre del taller:

Implementando seguridad en dispositivos capa 2

Objetivo de aprendizaje:

Desarrollar habilidades en el diseño e implementación de políticas de seguridad en dispositivos capa 2 con el fin de mitigar fallos de seguridad a partir de la implementación de hardening en dispositivos de redes Wi-Fi y redes LAN.

Descripción del taller:

En el presente taller se espera desarrollar habilidades en el diseño e implementación de la seguridad en dispositivos capa 2, iniciando con el control de accesos a los AP (*Access-point*) e implementando protocolos de seguridad en los mismos, al igual la aplicación de *hardening* en los *switch* de tal manera que de manera colectiva propongan políticas de red segura y confiable.

Requisitos para el taller:

- Realice la lectura del referente de pensamiento y de la lectura complementaria.
- Revise otros documentos asociados con la seguridad de AP y switch.
- Revise las videocápsulas propuestas en el eje.
- Lea con atención la rúbrica de evaluación.

Actividad
Evaluativa Taller

Instrucciones:

1. Realicen previamente la lectura del referente de pensamiento que aborda la seguridad en dispositivos capa 2.
2. Organicen grupos de máximo tres estudiantes.
3. Implemente la topología mostrada en el anexo.
4. Desarrolle la guía adjunta en el anexo.
5. Presente los resultados obtenidos en un documento. Recuerden ilustrar sus ideas con representaciones gráficas, así mismo integrar introducción, marco teórico, análisis de resultados, conclusiones grupales e individuales, metodológicas del ejercicio, bibliografía y el ejercicio funcional en *Packet Tracer*.
6. Envíe el documento en Word y el *Packet Tracer* al espacio de tareas del módulo.

Anexo Guía de taller a desarrollar

Taller implementación de seguridad en *Access point* y *switch*

Objetivo

Parte 1: Diseñar e implementar políticas de seguridad en redes LAN.

Parte 2: Configurar la seguridad del router Wi-Fi WRT 300N (AP).

Parte 3: Configurar la seguridad del switch.

Aspectos básicos

En esta actividad, configurará y verificará la seguridad de la red LAN propuesta, implementando *Hardening* en router Wi-Fi y *switch*.

Topología por implementar

La siguiente imagen muestra la topología a implementar en Packet Tracer, para el desarrollo del presente taller.

Actividad
Evaluativa Taller

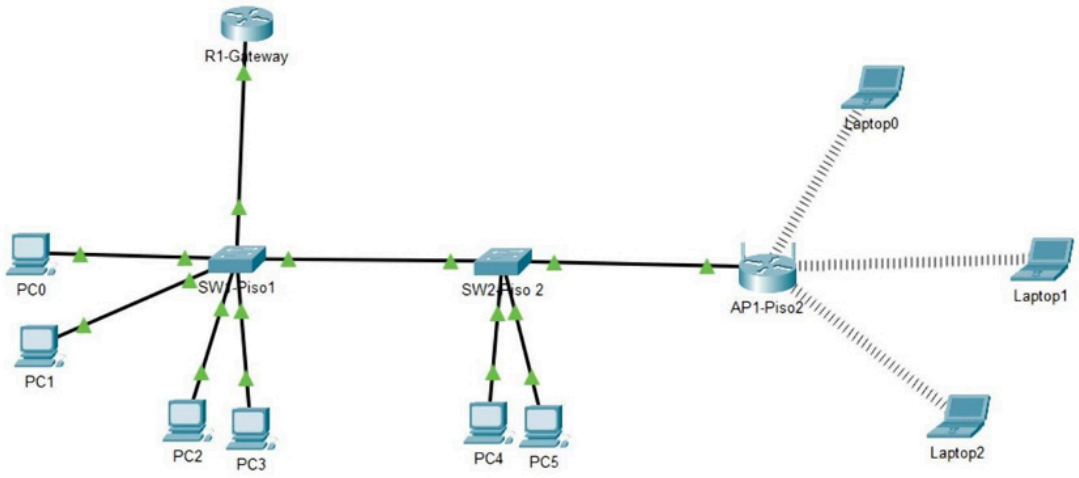

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara	Gateway
R1-gateway	G0/0/0.10	192.168.10.1	255.255.255.0	N/A
	G0/0/0.20	192.168.20.1	255.255.255.0	N/A
	G0/0/0.30	192.168.30.1	255.255.255.0	N/A
	G0/0/0.100	192.168.100.1	255.255.255.0	N/A
SW1-Piso1	VLAN 100	192.168.100.2	255.255.255.0	192.168.100.1
SW2-Piso2	VLAN 100	192.168.100.3	255.255.255.0	192.168.100.1
AP1-Piso2	IP LAN	192.168.50.1	255.255.255.0	N/A
AP1-Piso2	IP WAN	192.168.100.4	255.255.255.0	192.168.100.1
PC0	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC1	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC3	NIC	192.168.20.11	255.255.255.0	192.168.20.1
PC4	NIC	192.168.30.10	255.255.255.0	192.168.30.1
PC5	NIC	192.168.30.11	255.255.255.0	192.168.30.1
Laptop 0	NIC	DHCP	DHCP	DHCP
Laptop 1	NIC	DHCP	DHCP	DHCP
Laptop 2	NIC	DHCP	DHCP	DHCP

Actividad Evaluativa Taller

Tabla de VLAN

Rango de interfaz	# VLAN	Nombre de VLAN	IP VLAN
Interfaz f0/1-5	10	Compras	192.168.10.0/24
Interfaz f0/6-10	20	Ventas	192.168.20.0/24
Interfaz f0/11-15	30	TI	192.168.30.0/24
Interfaz f0/16-20	100	ADMIN	192.168.100.0/24
Interfaz f0/21-24	300	Parqueo	N/A

Paso 1: Implementar topología física y lógica

Diseñe en *Packet Tracer* el montaje de la red de acuerdo con la topología mostrada en la imagen y asigne direccionamiento de acuerdo con la tabla de direccionamiento.

Paso 2: Configuración de control de acceso y seguridad en al router WiFi

- Configure la red LAN y WAN del router WiFi de acuerdo con la tabla de direccionamiento.
- Implemente el control de acceso al router WiFi desactivando el SSID y cambiando el nombre al mismo.
- Desarrolle filtrado MAC de las tres Laptops ingresándolas a las listas de MAC permitidas.
- Aplique el protocolo de seguridad WPA2 al dispositivo router WiFi.
-

Paso 3: Configuración básica del switch

- Cambie el nombre a los switch según la tabla de direccionamiento.
- Agregue contraseña a modo privilegiado “FUAA123*”.
- Implemente un mensaje de advertencia.
- Cree dos usuarios con privilegio mínimo.
- Configure el acceso a SSH.

Paso 4: Configuración de VLAN

- Implemente las VLAN de acuerdo con la tabla de VLAN.
- Asigne dos PC a cada VLAN de acuerdo con la imagen y tabla de direccionamiento.
- Asigne los puertos a las VLAN de acuerdo con la tabla de VLAN.

Paso 5: Asegurando puertos

- Implemente la seguridad de los puertos para que admitan una única MAC
- Configure la acción shutdown cuando detecte una violación en el puerto.
- Configure la detección automática de la MAC en cada puerto.
- Implemente el DHCP snooping para prevenir ataques.

Paso 6: Análisis de seguridad de red

1. Explique qué beneficios de seguridad brinda a la red, el filtrado MAC y desactivar el SSID en un router WiFi.
2. Desarrolle un mapa mental sobre los protocolos de seguridad de la red WiFi, WEP, WPA, WPA2 y WPA3.
3. Proponga cómo podría mejorar la seguridad inalámbrica en el diseño implementado en el taller.
4. Explique la importancia de implementar la configuración básica de un dispositivo antes de colocar en producción.
5. Diseñe un mapa conceptual de los principales ataques a las redes LAN y las estrategias de mitigación.
6. Explique la importancia de implementar la seguridad en los puertos de switch.
7. Analice el impacto de la configuración de las VLAN en la seguridad de la red.
8. Desarrolle un cuadro comparativo entre Telnet y SSH.
9. Cuál es la importancia de implementar DHCP snooping en la red.
10. Proponga políticas de seguridad en red LAN que mejoren la seguridad, la alta disponibilidad y calidad de servicio de esta.

¡Éxitos!