

DATOS DE LA ACTIVIDAD							
No. de Actividad:	1.4	Actividad	Actividad Seguridad en Router Packet Tracer y Retroalimentación Router				
Unidad:	1: Riesgos de seguridad informática en infraestructura de red						
Carrera:	Tgo. en Desarrollo de Software						
Materia	Seguridad en ITI					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	Centro de Enseñanza Técnica Industrial plantel Colomos						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	19/02/2021
Compet. Genéricas		4.1, 4.5, 5.2, 5.5		Compet. Profesional		CP1-1	

1. Objetivo(s) de la actividad

- Identificar los comandos básicos que debemos implementar en la seguridad informática.

2. Instrucciones (Descripción) de la actividad

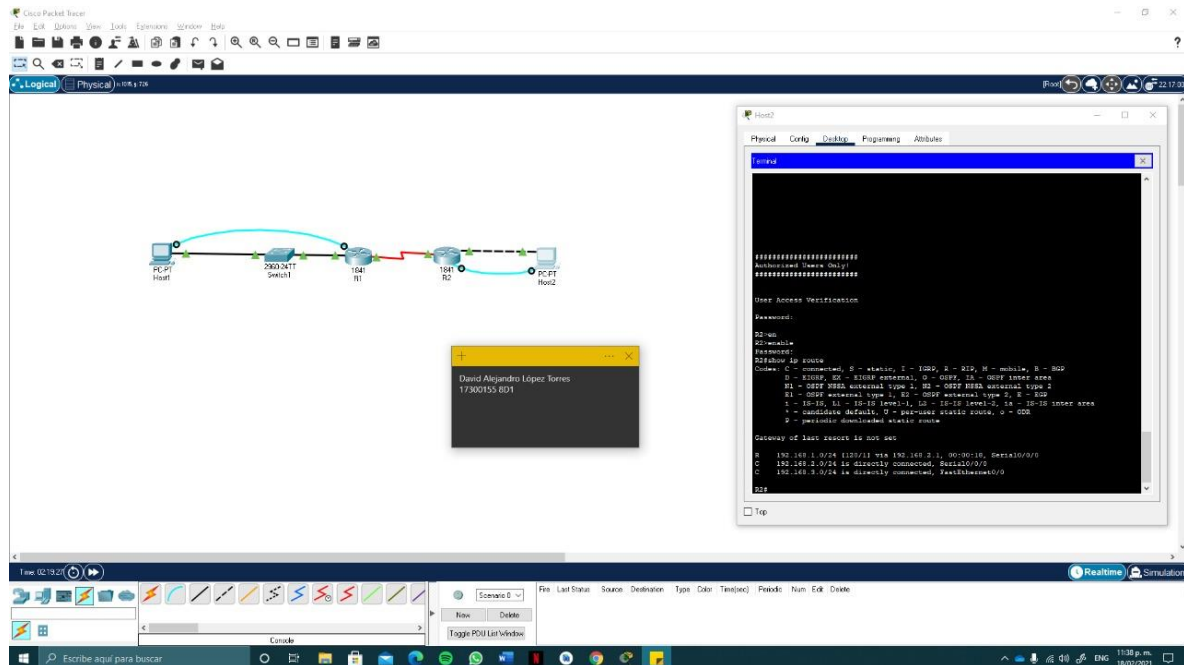
1. Usar el archivo PDF LAB 2355 para hacer la implementación de la topología ahí descrita en Packet Tracer y verificar el funcionamiento de la red.
2. Configurar en los Routers: las contraseñas seguras en la línea de consola, línea vty telnet y la línea auxiliar, la contraseña Enable Secret, configurar nombres de usuario de cuentas locales.
3. Verificar todos los comandos posibles indicados en el documento en el capítulo 2, páginas 52 a 85. Hacer una lista de comandos.
4. Tomar impresión de pantalla completa de la actividad, con su nombre

3. Desarrollo de la actividad

1	\$ (domain)
2	\$ (hostname)
3	\$ (line)
4	\$ (line-desc)

5	banner {exec incoming login motd slip-ppp} d message d
6	Cifrar Todas las Contraseñas
7	commands parser-mode {include include- exclusive exclude} [all] [interface
8	nombreinterfaz comando]
9	config-register 0x2102
10	configure terminal
11	copy running-config startup-config
12	copy startup-config running-config
13	crypto key generate rsa general-keys módulo modulus-size
14	crypto key zeroize rsa.
15	Deshabilitar Conexiones no Utilizadas
16	enable nivel
17	enable secret
18	Enable secret password
19	enable secret level 5 cisco5
20	enable view
21	enable view root.
22	EXEC privilegiado enable view
23	Exit
24	line aux
25	Línea de Consola
26	Líneas de Terminal Virtual
27	login block-for segundos attempts intentos within segundos
28	login delay segundos
29	login delay.
30	login local
31	login on-failure log [every login]
32	login on-success log [every login]
33	login quiet-mode access-class {acl-nombre acl-número}
34	Longitud de Caracteres Mínima
35	no service password-recovery
36	parser view nombre-vista superview
37	privilege exec level 5 ping
38	privilege modo {level nivel de comando reset} comando
39	secret contraseña-cifrada.
40	secure boot- config restore nombre-archivo.
41	secure boot-config

42	secure boot-image
43	security authentication failure rate tasa umbral log
44	service password-encryption



4. Reflexión:

La gran cantidad de configuraciones que puedan aplicarse para garantizar la seguridad de la información que viaja a través de una red es un reflejo de la importancia que tiene este campo en los diferentes contextos en donde es importante implementar una red ya sea local o remota. Con el desarrollo de esta práctica fue posible reafirmar los conocimientos que se abordaron durante las materias anteriores en el ámbito del manejo de redes y en mi caso pude recordar algunos detalles que había olvidado de aquellos ayeres. Es interesante ver como una red tan simple como la mostrada requiere de una labor interesante de implementación de seguridad para llegar a una garantía de cierto nivel de seguridad.

5. Referencias:

CISCO (n.d.). POST data. CISCO Networking Academy. Retrieved February 19, 2021. Recuperado desde: <https://www.netacad.com/portal/learning>