Comprensión de la Necesidad de las Redes de Computadoras y Seguridad en los Tiempos de Conectividad Absoluta

Autor: Jonathan R Sosa Lugo
Mentor: Ph.D Alfredo Cruz Triana
Departamento de Ciencia de Cómputos

Abstracto

Comprender redes, seguridad informática y cifrados es esencial en ciberseguridad. Brindar a los estudiantes de nivel superior herramientas y fundamentos clave les permite reconocer componentes básicos del tema y tomar conciencia sobre la importancia de proteger las redes. A través de métodos de seguridad técnicos, lógicos y cifrados, se fortalecen sus conocimientos. Además, este aprendizaje beneficia a los maestros, permitiéndoles enseñar redes y seguridad de manera efectiva. También podrán usar programas para simular redes e implementar medidas de seguridad. Adquirir estos conocimientos ayuda a los estudiantes a explorar diversas áreas de desarrollo profesional en ciberseguridad.

Introducción

Crear módulos para maestros de secundaria para ampliar su perspectiva sobre tecnología es una necesidad en nuestra comunidad. Muchos estudiantes de nivel superior consideran carreras tradicionales y tienen ideas erróneas sobre ciberseguridad, asociándola con actividades ilícitas como el “hackeo”. Sin embargo, la seguridad tecnológica implica proteger organizaciones y empresas contra ataques.

En la actualidad, estar conectados a una red es esencial, ya sea inalámbrica, por cable o mediante puntos de acceso. Es importante comprender su configuración y seguridad, tanto técnica como física, para dificultar la extracción de datos. Mecanismos como el cifrado convierten la información en un formato ilegible para protegerla. Es por esa razón, que podemos hablar de distintos mecanismos de seguridad general y en las redes el cortafuegos.

Trasfondo

Al introducir el tema de las redes y el cortafuego hubo un interés en saber en cómo funciona las redes en nuestra sociedad. Como es de conocimiento, las redes es la pieza clave de comunicación en el ambiente en el que vivimos. También, se puede decir que es la primera fila de ataques cibernéticos en estos tiempos. Ya que, al estar conectados en la red, los atacantes cibernéticos pueden tomar ventaja para hacer sus crímenes. Los registros confirman que, en el primer trimestre del año 2024, por semana han alcanzado 1,308 de ataques. Aproximadamente es un aumento de 28% del año 2023. Es por esa razón que debemos de instruir, informar y enseñar a nuevas personas que puedan contribuir a la seguridad de las redes en estos tiempos. Por otra parte, el término seguridad surgió en 1979, asociado al liberalismo y a la protección de individuos y colectivos frente a diversos riesgos. Esto llevó a la implementación de medidas para controlar amenazas en salud, crimen y defensa. Con el tiempo, el concepto evolucionó hasta referirse a la sensación de estar a salvo y libre de peligros. Más adelante, nació la seguridad informática o ciberseguridad, enfocada en la protección de datos y sistemas. Su objetivo es prevenir ataques, extorsión y vandalismo mediante programas especializados.

Problema

El principal objetivo de este proyecto es poder brindarle un conocimiento básico de las redes de comunicaciones y cortafuego. También conocimientos en seguridad, importancia de las contraseñas y cifrados populares para poder implementarlas en nuestro diario vivir. En adición, poder implementarlas en un ambiente de prueba donde la persona pueda tener una experiencia en configurar su red y poder hacer diferentes pruebas en su configuración. Donde se le ofrecerá una guía sobre el programa común en las pruebas de redes.

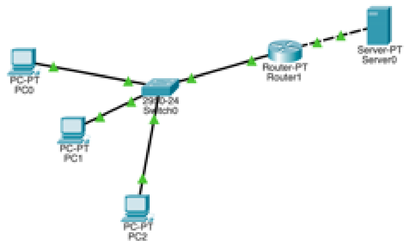
Metodología

En un tutorial de diseño en un programa de simulaciones de redes va a hacer pieza clave en la enseñanza y soluciones de problemas de las redes. Donde se va a poder adquirir destrezas de topologías, conexiones por cable o inalámbricas, configuraciones, y destrezas sobre programas importantes sobre redes como Telnet e interfaz de línea de comandos. Dichos programas que vienen integrados en una computadora hacen que nos familiaricemos para análisis de la computadora hasta respuestas de accidentes que son importantes en la seguridad cibernética. En adición, hace una contribución a las redes de computadoras de una forma técnica, sencilla y de aprendizaje.

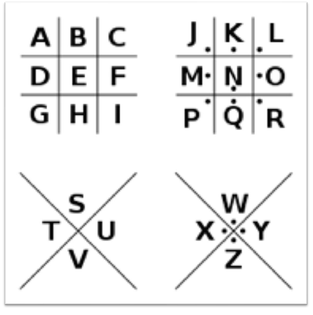
En la parte de la seguridad vamos a seleccionar cuatro cifrados populares para poder brindar conocimientos básicos y encontrar escenarios pertinentes a la hora de su implementación. En adición, mencionar métodos de criptografía para asegurar la confidencialidad, integridad y autenticación de los datos en nuestro lugar de trabajo o documentos personales.

El escenario de la prueba para el programa de Cisco Packet Tracer constara de hacer una configuración de tres computadoras personales, un conmutador, un enrutador y un servidor. Donde en el enrutador va a hacer capaz de hacer el trabajo del cortafuego.

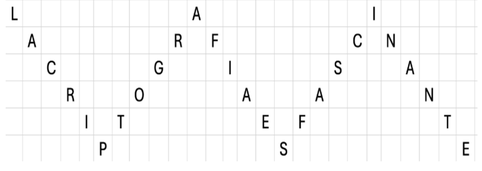
Para los problemas del cifrado de Pigpen, Railfence, Playfair, y Vernam no necesitamos ningún tipo de programa para hacer uso de dichos cifrado. Simplemente comprender como es que trabajan cada uno de ellos para poderlos implementar en el área que se necesite implementar.



Gráfica 1 Topología del Cortafuego



Gráfica 2 Distribución del Abecedario Pigpen



Gráfica 3 Encriptación con el Método Railfence

Resultados y Discusiones

Los resultados sobre la simulación de una topología con una configuración de IP y cortafuegos fueron realizados con éxito. Desde la interface del programa hasta los componentes virtuales fueron posibles en completar dicha simulación.

Se empezaron a configurar las computadoras personales asignándoles direcciones IP, mascará de subred, y la puerta de enlace predeterminada.

En la implementación del cortafuego, la vamos a implementar en el enrutador donde el terminal va a tener la configuración pertinente para que pueda realizar el trabajo. En la configuración debe existir el acceso negado o permitido del protocolo de comunicación que la persona desee. Por ejemplo, si desea negar la comunicación ICMP debe de contener la siguiente sintaxis “access-list 101 deny icmp” para poder restringir el acceso.

Al hacer la simulación con la restricción del protocolo de comunicación ICMP, vemos que se puede comunicar con las demás computadoras personales, pero no entra al enrutador, haciendo posible la función del cortafuego, no permitir lo que el programador de la red estableció que tipo de comunicación puede entrar a la red configurada.

En los escenarios de cifrado, pudimos comprobar la utilidad de los métodos explicados, observando cómo un mensaje podía ser cifrado siguiendo las reglas correspondientes. Es importante notar que los resultados pueden variar dependiendo del mensaje que se encripte.

Cisco Packet Tracer es una herramienta clave para estudiantes y profesionales interesados en redes de comunicación. Además, organizaciones como las fuerzas aéreas la utilizan para entrenar a su personal en la configuración de dispositivos, ya que, al ser productos de Cisco, facilita una transición rápida, efectiva y segura a los componentes reales en el entorno laboral.

Tabla 1 Distribución de Direcciones IP en Computadoras Personales

Computadoras personales	Direcciones IP	Mascará de subred	Puerta de enlace predeterminada
PC0	192.168.15.2	255.255.255.0	192.168.15.1
PC1	192.168.15.3	255.255.255.0	192.168.15.1
PC2	192.168.15.4	255.255.255.0	192.168.15.1
Server0	223.223.223.2	255.255.255.0	

Tabla 2 Resultado de la Palabra Encriptada Azul con Método Vernam

Valor hexadecimal	Operación XOR	Clave de la letra	=	Resultado en binario	Resultado en ASCII
0100 0001	⊕	1011 0110	=	1111 0111	/
0101 1010	⊕	1100 1001	=	1001 0011	“
0101 0101	⊕	1110 0010	=	1011 0111	·
0100 1100	⊕	0110 1101	=	0010 0001	!

Conclusión

Cisco Packet Tracer es una herramienta clave para el aprendizaje en redes, seguridad informática y criptografía. Cisco, líder en el diseño de servidores, enrutadores y conmutadores, ha consolidado su simulador como una plataforma esencial para practicar configuraciones de dispositivos de red, facilitando la adquisición de habilidades aplicables en entornos laborales.

Más allá de las conexiones físicas y configuraciones básicas, permite explorar aspectos avanzados como segmentación de redes, protocolos de seguridad y cifrado de datos. En un mundo donde la ciberseguridad es crucial, esta herramienta ayuda a garantizar la confidencialidad, integridad y autenticidad de la información.

Además, simula escenarios reales, como cortafuegos con cifrado, VPNs seguras y detección de amenazas, preparando a los usuarios para el ámbito profesional. Su uso continuo impulsa el desarrollo en ciberseguridad, diseño de redes y criptografía, posicionando a los usuarios como profesionales altamente competitivos en el mercado laboral.

Trabajos Futuros

En el futuro, podríamos desarrollar mecanismos de defensa para detectar anomalías en redes, fortalecer la seguridad con autenticación y VPNs, simular ataques para mejorar la respuesta y aplicar políticas de seguridad según niveles de acceso.

Cisco Packet Tracer sigue siendo una herramienta clave para innovar y probar redes. Además, la creación de sistemas inteligentes que automaticen la gestión de claves criptográficas mejoraría la seguridad, reduciendo errores humanos y agilizando procesos en infraestructuras complejas.

Agradecimientos

Primeramente, le quiero dar las gracias a Dios por haberme dado la sabiduría y el entendimiento para poder cumplir con los estándares estipulados en el proyecto. También, a mi mentor el Dr. Alfredo Cruz Triana por guiarme y darme las sugerencias correspondientes para hacer un trabajo de excelencia. Siempre pendiente de sus estudiantes para cumplir sus metas profesionales en el mundo de la seguridad informática. Gracias a mi familia y amistades por empujarme a seguir desarrollándome profesionalmente.

Referencias

- Kaspersky, "¿Qué es un firewall y cómo funciona?," Kaspersky, 2024. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/firewall. [Accedido: 10-nov-2024].
- Secureframe, "Cybersecurity Statistics: 2024 Trends, Data, and Insights," Secureframe, 2024. [En línea]. Disponible en: https://secureframe.com/es-es/blog/cybersecurity-statistics. [Accedido: 10-ene-2025].
- CCNA Desde Cero, "¿Qué es Cisco? Historia y evolución," CCNA Desde Cero, 2024. [En línea]. Disponible en: https://ccnadesdecero.es/que-es-cisco-historia/. [Accedido: 30-oct-2024].
- Cisco Systems, "Understanding Subnet Masks," Cisco Documentation. [En línea]. Disponible en: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13790-8.html [Accedido: 11-ene-2025].
- E. Raffino, “Seguridad,” *Enciclopedia Concepto*, 2023. [En línea]. Disponible: https://concepto.de/seguridad/ [Accedido: 24-feb-2025]
- E. Prieto, “¿Cuál es la historia de la ciberseguridad?,” *Saint Leo University*, Jun. 21, 2024. [En línea]. Disponible: https://worldcampus.saintleo.edu/blog/historia-de-la-ciberseguridad/ [Accedido: 24-feb-2025]