RESUMEN

La presente propuesta pretende observar el comportamiento de los diferentes mecanismos de seguridad que se pueden implementar a nivel de capa 3, los cuales puede ser adoptados por los proveedores de servicios y las diversas empresas que requieran este servicio, con la finalidad de que la información o los datos se transmitan de manera confiable y segura. Para estos mecanismos de seguridad se requiere que tengan una conexión de mallado completo, para que la transmisión de paquetes se desarrolle de manera óptima y adecuada, el mecanismo de seguridad tradicional IPSec es un mecanismo que funciona punto a punto, mientras que GETVPN es un mecanismo que realiza un trabajo multipunto multipunto. Mediante el software GNS3 que permite simular redes de esta magnitud, se realizó la experimentación con diferentes escenarios, identificando la seguridad y funcionamiento en una red MPLS con servicio de VPNs, además de una pequeña prueba de penetración o auditoría de red que permite saber que tan seguro se encuentra a un ataque de intrusión real. En la prueba de pentesting se ejecuta mediante una máquina virtual, que contienen el software Kali Linux, teniendo una conexión con GNS3, utilizando esta herramienta se realiza la prueba de penetración en la cual se observa la robustez y seguridad del sistema.

Palabras Claves:

PROTOCOLO DE ETIQUETAJE

SOFTWARE DE SIMULACIÓ REDES DE COMUNICACIÓN

PROTOCOLOS DE ENCRIPTACIÓN DE DATOS

REDES PUNTO - MULTIPUNTO

AUDITORÍA SEGURIDAD INFORMÁTICA

ABSTRACT

The present proposal aims to observe the behavior of the different security mechanisms that can be implemented at layer 3 level, which can be adopted by the service providers and the various companies that require this service, in order that the information or The data is transmitted reliably and safely. For these security mechanisms it is required that they have a full meshing connection, so that packet transmission is optimally and adequately developed, the traditional IPSec security mechanism is a point-to-point mechanism, where as GETVPN is a mechanism Which performs a multipoint multipoint job. Using GNS3 software to simulate networks of this magnitude, experimentation with different scenarios was performed, identifying security and performance in an MPLS network with VPN service, as well as a small penetration test or network audit, Securely encountered a real intrusion attack. In the test of pentesting is executed by means of a virtual machine, that contains the software Kali Linux, having a connection with GNS3, using this tool the penetration test is realized in which the robustness and security of the system is realized.

Keywords:

LABEL PROTOCOL

SOFTWARE SIMULATION COMMUNICATION NETWORKS

DATA ENCRYPTION PROTOCOLS

POINT- MULTIPOINT NETWORKS

COMPUTER SECURITY PENTESTING