TALLER SEGURIDAD DE REDES DE DATOS

A continuación encontrará un taller que le ayudará como preparación para la presentación del Examen Final Teórico de Seguridad de Redes de Datos. Durante esta Actividad podrá utilizar el material compartido en drive de temas asignados por el instructor realizado por los aprendices o material de la curricula de Cisco suministrado por el instructor u otras fuentes de estudio, al igual lo podrá desarrollar en grupo de Máximo 3 personas.

El taller está centrado en la parte de diferenciación de conceptos que están muy asociados y se cree una diferenciación clara entre componentes que pueden ser muy parecidos. Si lo desea lo puede trabajar de forma individual para mayor apropiación de conocimiento.

LAN

1) En una tabla comparativa defina las diferencias que tiene STP y RSTP en cuanto a estados, tipos de puertos y tiempos. En cuanto a VTP defina la diferencia entre sus 3 modos VTP.

2) De acuerdo con lo visto en HSRP, GLBP, y VRRP, realice una tabla comparativa en donde plantee claramente las diferencias y similitudes entre estos protocolos.

3) Defina la importancia de NTP y Syslog, mencione los niveles de Syslog, de ejemplos de configuración de estos. Finalmente realice una tabla dando una breve descripción de NTP, Syslog.

4) Teniendo claro los conceptos de la agregación de enlaces por medio de EtherChannel, realice una tabla comparativa en donde plantee claramente las diferencias y similitudes entre los protocolos de negociación que EtherChannel maneja. (mencione sus modos y diferencias).

5) Defina la diferencia de trabajar ssh con autenticación login local y utilizar ssh con autenticación en un servidor Radius. (anexe como serían los comandos para la configuración de estos 2 tipos de autenticación).

6) En redes inalámbricas realice una tabla donde defina claramente cuales son métodos de cifrado, métodos de encriptación y algoritmos de cifrado, de una breve descripción de cada uno de estos.

7) De los temas planteados en este módulo de seguridad defina qué solución es la que me brinda cada uno de los temas aprendidos, STP, RSTP, EtherChannel, Snooping, PortSecurity, entre otros. De una pequeña descripción de la importancia de su uso.

WAN

8) Teniendo claro los conceptos relacionados con las ACL, realice una tabla comparativa en donde plantee claramente las diferencias y similitudes entre las ACL estándar y extendidas, y entre las numeradas y nombradas.

9) Dentro de la terminología de VPN se maneja diferente terminología, realice una tabla donde clasifique los protocolos utilizados para autenticación, integridad, confidencialidad, y seguridad de claves.

10) Mencione la diferencia entre las VPN de acceso remoto y la sitio a sitio, realice la misma operación con los tipos de NAT, realice énfasis en la sintaxis del comando de los tipos de NAT y para hacia qué tipo de topología va dirigido.

11) Para la creación de ACL es fundamental manejar muy bien tanto los números de puertos, como el protocolo de capa de transporte utilizado, realice una tabla donde defina al menos 10 protocolos de la capa de aplicación, seguido de su puerto y el protocolo de capa de transporte que utiliza.

12) Teniendo claro los conceptos teóricos principales de NAT realice en PKT una topología sencilla en donde se vea un ejemplo claro de NAT. Por medio de las notas de pkt asigne direcciones IP, y defina cuál sería la Local interna, Global interna, Local externa y Global Externa. (adjunte la imagen de la Topología, no se configura, solo se necesita la topología).

13) Defina el rango de direcciones IP privadas, e ingrese al menos 10 ejemplos de IP privadas y 10 de IP públicas, también al final mencione cuando una IP se puede considerar como inválida a la hora de ingresarla a un PC.

14) Ingrese al menos 2 ejemplos sencillos de ACL nombrada (1 estándar y 1 extendida), realice lo mismo con las numeradas. (Observe bien y explique la sintaxis). Realice el mismo procedimiento ingresando al menos 1 ejemplo de NAT estático, 1 de dinámico, 1 de dinámico sobrecargado y 1 de PAT por única IP. (Ejemplo por medio de comandos).

15) Defina los pasos correctos para crear una VPN IKEv1, desde la configuración, hasta la verificación de esta. Mencione inicialmente los pasos de forma general, y finalmente ingrese un ejemplo de esta configuración.

16) Cree una tabla comparativa de los protocolos que se manejan en IPsec (AH y ESP) mencione estos cuales protocolos pueden usar para autenticación, integridad y confidencialidad.

17) Mencione los diferentes tipos de violación que maneja Port-Security, defina cada una de ellas y de un ejemplo de estas (comandos). De igual manera mención diferencias entre port-security estático y dinámico. (de un ejemplo con comandos).

18) Realice una tabla completa donde se asocie cada sigla utilizada durante este módulo con su respectiva definición, algunos ejemplos de estas son (AES, SHA, MD5, PSK, SHA, IKE, ACL, NAT, VPN, STP, VTP, ASA, entre otros).

Una vez finalizado, guarde el documento en formato PDF con su nombre en la portada, y finalmente proceda a subirlo a Territorium a más tardar un día antes del Examen.