DEBILIDAD DE LOS PROTOCOLOS TCP/IP

Sku: 3887EC

Horas: 10

OBJETIVOS

Analizar la seguridad de las comunicaciones. Enumerar y desarrollar los mecanismos de seguridad de redes y los protocolos de autenticación. Clasificar y desarrollar, las comunicaciones de voz segura, la ingeniería social y las amenazas de fraude y abuso. Conocer cómo administrar la seguridad del correo electrónicos, los objetivos, problemas y soluciones de seguridad llevadas a cabo. Definir los términos relacionados con la red privada virtual, virtualización y NAT. Desarrollar las características que componen el control de seguridad.

CONTENIDOS

1. COMUNICACIONES SEGURAS 2. MECANISMOS DE SEGURIDAD DE REDES Y PROTOCOLOS 2.1. PROTOCOLOS DE COMUNICACIONES SEGURAS 2.2. PROTOCOLOS DE AUTENTICACIÓN 3. COMUNICACIONES DE VOZ SEGURAS 3.1. VOZ SOBRE PROTOCOLO DE INTERNET (VOIP) 3.2. INGENIERÍA SOCIAL 3.3. FRAUDE Y ABUSO 4. COLABORACIÓN MULTIMEDIA 4.1. REUNIÓN REMOTA 4.2. MENSAJERÍA INSTANTÁNEA 5. ADMINISTRAR LA SEGURIDAD DEL CORREO ELECTRÓNICO 5.1. OBJETIVOS DE SEGURIDAD DE CORREO ELECTRÓNICO 5.2. ENTENDER LOS PROBLEMAS DE SEGURIDAD DE CORREO ELECTRÓNICO 5.3. SOLUCIONES DE SEGURIDAD DE CORREO ELECTRÓNICO 6. GESTIÓN DE SEGURIDAD DE ACCESO REMOTO 6.1. PLANIFIQUE LA SEGURIDAD DEL ACCESO REMOTO 6.2. PROTOCOLOS DE ACCESO TELEFÓNICO 6.3. SERVICIOS DE AUTENTICACIÓN REMOTA CENTRALIZADA 7. RED PRIVADA VIRTUAL 7.1. TÚNEL 7.2. CÓMO FUNCIONAN LAS VPN 7.3. PROTOCOLOS VPN COMUNES 8. LAN VIRTUAL 9. VIRTUALIZACIÓN 9.1. SOFTWARE VIRTUAL 9.2. REDES VIRTUALES 10. TRADUCCIÓN DE DIRECCIONES DE RED 10.1. NAT CON ESTADO 10.2. NAT ESTÁTICO Y DINÁMICO 10.3. DIRECCIONAMIENTO IP PRIVADO AUTOMÁTICO 11. CARACTERÍSTICAS DE CONTROL DE SEGURIDAD 11.1. TRANSPARENCIA 11.2. VERIFICAR INTEGRIDAD 11.3. MECANISMOS DE TRANSMISIÓN 12. LÍMITES DE SEGURIDAD