

# LECTURA CAPITULO 5 Y 6



Yanet Islas Yañez

ITI 91

Aplicación de  
Telecomunicaciones

MTI. Oscar Lira Uribe

# Seguridad y Monitoreo de Red

## Ataque de Fuerza Bruta

Un atacante utiliza reiteradamente una lista de contraseñas comunes. Con el tiempo suficiente y dado las condiciones propicias, un ataque de contraseña por fuerza bruta puede descifrar casi cualquier contraseña.

## Estándar IEEE 802.1X

Define un control de acceso y un protocolo de autenticación basado en puertos.

## Ataque de DoS por Telnet

Hay varias maneras de mitigar los ataques de Telnet:

- Use SSH en vez de Telnet para las conexiones de administración remota.
- Use contraseñas sólidas y cámbielas con frecuencia. Una contraseña segura debe tener una combinación de mayúsculas y minúsculas, y debe incluir números y símbolos (caracteres especiales).
- Limite el acceso a las líneas de vty con una lista de control de acceso (ACL) que permita el acceso sólo a los dispositivos de administrador y deniegue el acceso a todos los demás.

## Ataque de desbordamiento de tabla CAM

Bombardeando el switch con direcciones MAC falsas hasta que la tabla de direcciones del switch se llena.

## Protocolo simple de Administración de Red

Software que crea y ejecuta instancias de MV.

## Ataque por suplantación de Identidad del DHCP

Un atacante configura un servidor DHCP falso en la red para emitir direcciones DHCP para los clientes. Este tipo de ataque obliga a los clientes a usar un servidor falso de sistema de nombres de dominio (DNS)

## Elementos en la Implementación de SNMP

Agentes de SNMP (dispositivos administrados) base de información de administración (MIB).

## Ataque por Agotamiento de Direcciones DHCP

Una vez que se emiten estas direcciones IP, el servidor no puede emitir más direcciones; esta situación produce un ataque por denegación de servicio (DoS), ya que los nuevos clientes no pueden obtener acceso a la red.

# Calidad del Servicio

## Congestión de la Red

El pedido de ancho de banda de red excede la cantidad de ancho de banda disponible.

## Configuración de Colas

Los paquetes se pueden almacenar temporalmente en la memoria con buenos recursos disponibles.

## Ancho de Banda de Red

La cantidad de bits que se pueden transmitir en un solo segundo (bps).

## Demora/Latencia

El tiempo que tarda un paquete en viajar de un origen a un destino.

## Fluctuación de Fase

La variación del tiempo que tarda un paquete en viajar de un origen a un destino.

## Tráfico de Voz

La voz es muy sensible a las demoras y los paquetes descartados; no hay motivo para retransmitir la voz si se pierden paquetes.

## Tráfico de Video

Es menos resistente a pérdidas y tiene un mayor volumen de los datos por paquete. Si la transmisión de video se compone de contenido que no cambia mucho de un cuadro a otro, los paquetes de video serán pequeños, y se necesitarán menos para mantener una experiencia de usuario aceptable.

## Clasificación o Marcado

Para determinar la clase de tráfico a la que pertenece este paquete.

## Prevención de Congestión

Cuando la cola alcanza el umbral máximo, se descarta un pequeño porcentaje de paquetes para prevenir la congestión.