“Secretaria De La Educación Superior”

“Instituto Tecnológico de Cancún”

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Investigar sobre MITM

Alumno: Vargas Rodríguez Javier Jesús

Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 12/Noviembre/2020

Horario: 5:00 pm – 6:00 pm

Investigar sobre MITM

¿QUÉ ES UN MAN IN THE MIDDLE O MITM?

Un ARP Poisoning es uno de los métodos más comunes de ataques a redes, y que permite llevar a cabo un MITM. Lo que se busca es que el caché de la máquina o máquinas que queremos registrar tengan como dirección MAC la del atacante, y mantengan la dirección IP real de una de las máquinas de la red. Con esto, todo el tráfico que circule por esa red en dirección a esa IP (o no) pasará antes por el terminal atacante, y podrá ser leído, modificado o borrado.

Los ataques Man in the middle o MITM no solo se usan entre terminales conectados en la misma red, sino que también podría usarse para comunicaciones en varias redes mediante routers.

Existen varios métodos para defenderse de un Man in the middle o MITM, aunque por lo general, el mayor problema es enterarte. Para ello, existen algunos posibles efectos que hay que tener en cuenta, aunque ninguno es 100% efectivo, y habrá que recurrir a software o a un análisis ARP para saberlo a ciencia cierta.

Pero si lo que queremos es una defensa a posibles ataques MITM, existen dos métodos:

Tablas ARP estáticas: Los MITM existen gracias al ARP Poisoning, y éste gracias a que el caché ARP se actualiza dinámicamente.

Para evitar esto, bastaría con que las tablas caché de ARP sean estáticas. Pero como todo en esta vida, no es la panacea, ya que, si el caché es estático, cualquier cambio en la dirección de uno de los terminales tendrá que ser actualizada a mano en todos los demás, por lo que este método, aunque infalible, solo se usa en redes pequeñas, fácilmente operables por un único administrador.

DHCP snooping: El protocolo de configuración dinámica de host hace exactamente eso, ofrecer dinámicamente una configuración a cada terminal.

En esencia, este tipo de arquitectura es más segura y cómoda (ya que se actualiza sola), por el simple hecho de que un nuevo terminal es fácilmente reconocible en el historial, pero tiene asociado otro ataque como puede ser el de la clonación de DHCP, esto es, montarse un DHCP falso conectado en red que conteste a las peticiones DISCOVERY.

El que primero conteste (el falso o el verdadero) será el que administre la configuración de los terminales. Afortunadamente, dos DHCP activos cantean mucho, y bastaría activar Wireshark (u otro software de registro semejante) para ver qué IPs devuelven OFFER