Práctica Nº 4: Sniffers

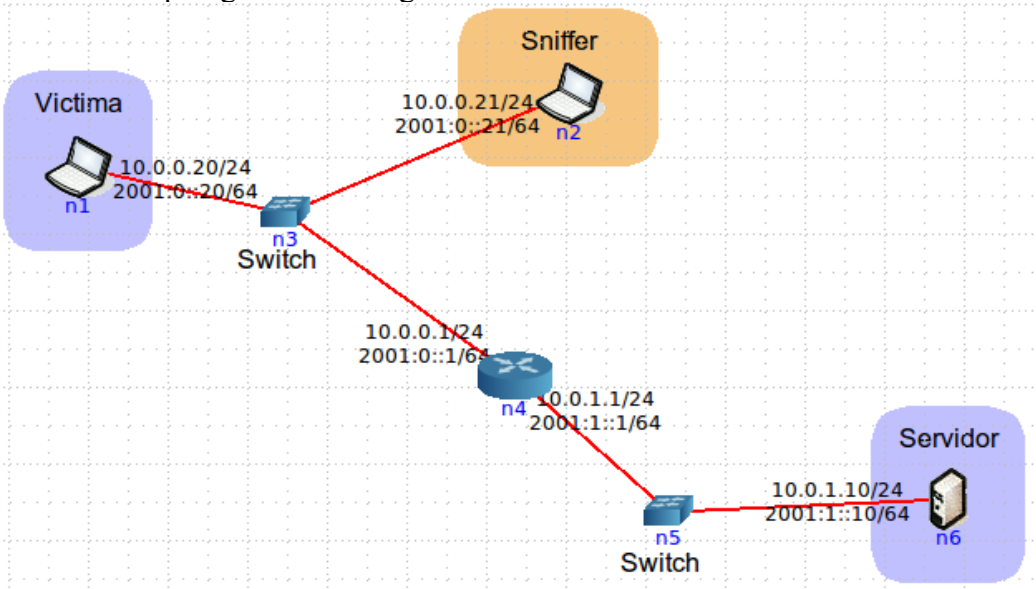
1. ¿Qué son los sniffers? ¿Para qué se los puede utilizar?

2. ¿Qué diferencias existen entre un sniffer y un analizador de protocolos?

3. Mencione herramientas que pueden ser utilizadas para sniffear. Pruebe la funcionalidad de alguna de ellas.

4. Mencione servicios que transmiten información sensible en texto plano. Utilice alguno de los sniffers analizados previamente a fin de obtener información sensible de estos. Defina y aplique filtros a las capturas que realice para visualizar mejor los datos capturados.

5. Sniffing en redes switcheadas:
   (a) Ejecute la aplicación "**core**". Inicio → ejecutar → core
   (b) Cree una topologia como la siguiente:



   (c) Inicie la virtualización con el boton verde de play.

   Una vez iniciada la virtualización, puede ingresar a cada dispositivo clickeando con el botón derecho sobre el dispositivo → shell windows → bash

   (d) Verifique el funcionamiento de la red realizando un **ping** desde la estación víctima hacia el servidor. Deje el **ping** corriendo indefinidamente.
   (e) Utilice en la estación sniffer **tcpdump** para verificar que no puede escuchar el trafico intercambiado entre la víctima y el servidor.
   (f) Paralelamente, abra otras shell bash en la estación sniffer para manipular el protocolo ARP con el comando **arpspoof** para poder capturar tanto el trafico de la víctima al servidor como el del servidor a la víctima. Puede ser necesario configurar la estación sniffer para forwardear el trafico. Esto se realiza con el comando:
   echo 1 > /proc/sys/net/ipv4/ip_forward
   (g) Luego del ataque, la víctima podría darse cuenta del mismo por la aparición de los ICMP redirects. Investigue qué son, por-qué aparecieron y cómo puede configurarse la estación

sniffer para que no los mande.

(h) Una vez logrado lo anterior, utilice el comando **tcpdump** en la estación víctima para analizar el trafico ARP de la LAN con el objeto de identificar el comportamiento malicioso por parte de la estación sniffer.

6. Busque y pruebe sniffer de propósito específicos que permitan capturar diversos tipo de información: chats, mensajería instantánea, imágenes en tráfico HTTP, contraseñas en distintos protocolos que viajan sin encripción, etc.

7. ¿Qué métodos existen para detectar un sniffer?

8. Busque e instale herramientas que detecten sniffers. Pruébelas y analice su efectividad.

9. ¿Qué significa MITM?

10. ¿Que permite hacer SSLstrip? Pruebe su funcionamiento en un entorno de pruebas controlado por usted.

11. ¿Qué son los keyloggers? ¿Qué tipos de keyloggers existen? ¿Para qué se los utiliza? ¿Cómo pueden distribuirse los mismos?

12. Busque y pruebe algún keylogger. Describa la funcionalidad del mismo.

13. ¿Como pueden detectarse los keyloggers?

14. Dado las siguientes formas de realizar un ataque de phishing contra un usuario que utiliza el homebanking https://www.mibanco.com
    (a) Usuario víctima de la recepción de un mail institucional del banco con un link que lo lleva a http://www.banco.com/mibanco/
    (b) Usuario víctima de la recepción de un mail institucional del banco con un link que lo lleva a https://www.banco.com/mibanco/
    (c) Instalación malintencionada por parte de un tercero del certificado de CA implementada por el atacante para emitir y configurar en el sitio https://www.banco.com/mibanco/ un certificado de dicha CA. Posteriormente, el usuario es víctima de la recepción de un mail institucional del banco con un link que lo lleva a https://www.banco.com/mibanco/
    (d) Manipulación del archivo de hosts de la PC del usuario para que www.mibanco.com tenga la IP del servidor del atacante.
    (e) Víctima de ataque de sslstrip cuando ingresa a su homebanking a traves del sitio http://www.mibanco.com el cual lo redirige luego a https://www.mibanco.com
    (f) En caso que imagine otra forma alternativa, describa su funcionamiento y compárela con las otras.

    Para cada caso:
    1. ¿Que mecanismo tiene el usuario para darse cuenta que se trata de un ataque?
    2. ¿Que acciones podría tomar el usuario o la organización, dependiendo del caso, para evitar que el usuario sea víctima del ataque en caso de que éste quiera ingresar al sitio de homebanking?