Seguridad en TI (TICS413)
Laboratorio n°2

Matías García
matiasgarcia@alumnos.uai.cl

26 de Agosto 2025

1.- Seguridad en redes

1.1.- Los riesgos de la red

En el presente se han conocido demasiados ataques a la seguridad de nuestros equipos a traves de las redes y se usan distintos metodos para conseguirlo. Se pueden segmentar en tres tipos generales de ataques:

- `Ataques Físicos`: Relacionados con el acceso directo a la infraestructura (instalación de malware malicioso, corte de cables de red o fibra óptica, robo o manipulación de equipos, acceso no autorizado a una habitacion como los servidores).
- `Ataques Técnicos`: Uso de vulnerabilidades en protocolos, sistemas o configuraciones (intercepción de datos, ataques de disponibilidad[DoS o DDoS], explotación de vulnerabilidades, malware de red, abuso de mala configuración).
- `Ataque de Ingeniería Social`: Explota el factor humano para obtener acceso a un sistema o red (Phishing [correos falsos],Vishing [llamadas falsas], smishing [sms falsos], Pretexting [cuento del tio], Shoulder surfing [mirar por encima del hombro], Tailgating [forzar la entrada física a un área restringida siguiendo a alguien autorizado])

Un ataque a la seguridad no solo es 1 de esos 3 tipos, sino que puedes ser una combinación de 2 o de los 3. Por ejemplo el "Man in the Middle" puede ser unicamente Ing. Social (si es que usa correo, llamada o shoulder surfing) pero se puede combinar con un ataque Tecnico un ejemplo seria:

Clonar la conexión wifi, almacenar toda la información que vaya por trafico en esa red y usarlo para acciones maliciosas.

Con este ejemplo podemos ver la combinación y ver lo "facíl" que seria lograr esta combinación

1.2.- The Man in the middle

"The man in the middle" o "el hombre del medio" es un riesgo de tipo "`intercepción de datos`" (en algunos casos puede ser manipulación y/o disponinilidad), ya que el atacante

se coloca entre dos puntos de una comunicación para **leer, modificar o redirigir** la información sin que las partes se den cuenta de estos actos.

Hay que dejar claro que no todo rastreo corresponde a esta categoria de MITM (Man in the middle), esto solo aplica cuando las acciones del tercero son maliciosas o tu no has dado consentimiento para este rastreo (El caso presentado por Edward Snowden es un ejemplo).

2.- Analizadores de protocolos de red - Network Protocol Analyzer (NPA)

Los analizadores son Herramientas que permiten Capturar, inspeccionar y analizar el tráfico que circula por una red en tiempo real o desde archivos previamente guardados. Su función prinicipal es descomponer los paquetes de datos captados que se transmiten entre dispositivos, mostrando de forma dettalada la información de cada protocolo utilizado (como puede ser TCP, HTTP, DNS, etc). esto permite a los administradores de red, ingenieros de seguridad y desarrolladores diagnosticar problemas, verificar configuraciones, analizar comportamiento sospechosos o realizar auditorías. Una de las más usada dentro de esta categoría es Wireshark.

2.1- Wireshark

Es una herramienta para NPA, permite inspeccionar cada paquete con detalle, mostrando información sobreprotocolos, direcciones IP, puertos y contenido. Su interfaz gráfica es intuitiva y facilitael filtrado y la búsqueda de datos relevantes, lo que la convierte en una herramienta útil tanto para profesionales como para estudiantes. Se emplea comúnmente para diagnosticar problemas de red, analizar el funcionamiento de aplicaciones y detectar comportamientos anómalos.

3.- Asociación entre seguridad y redes

Lo que ocurre con todo lo mencionado es ¿como asocio redes con la seguridad mas haya que coloquen un "virus" en el router? Para eso se generó esta sección.

La gente no siempre buscará encontrar tus claves o robar tu cuenta de banco, mcuchas veces lo que van a querer es información simple (que buscas, que ves, que consumes, que lugares visitas, etc), y en parte se puede conseguir esa información por medio de tu trafico en un red privada o publica, ya que en esta red se puede ver tus paquetes (tanto tcp como udp). Y para poder verlos tenemos el Wireshark y asi descubriremos un poco mas de la persona que queremos atacar.

4.- Práctico

Utiliza los computadores del laboratorio de ciberseguridad, sede Viña del Mar, dentro de Kali linux localiza la aplicación Wireshark y abrelo, empieza a ver como funciona y que se puede hacer.