PRÁCTICA EVALUABLE 2

Seguridad en la Información

Lenguajes y Ciencias de la Computación.
ETSI Informática, Universidad de Málaga

EJERCICIO 1: Análisis de protocolos (3,5 puntos)

En el Campus Virtual tienes una captura de tráfico llamada `captura.pcapng`. También la tienes disponible en CloudShark:

https://www.cloudshark.org/captures/5ec9b0601bcd

Se pide responder a las siguientes preguntas:

1. ¿Cuántas conexiones TLS se establecen y con cuantos servidores diferentes? ¿Qué filtro de Wireshark te permite responder fácilmente a esta pregunta?
2. ¿Qué versión de TLS se utiliza en la conexión con el host 150.214.108.1? ¿Y con el host 150.214.40.78?
3. ¿Existe alguna conexión TLS 1.3? En caso afirmativo indica con qué host.
4. En la conexión con el servidor 20.189.173.14, ¿qué suites de cifrado se ofertan al servidor? ¿cuál es la elegida para establecer la conexión?
5. ¿Cuál es la clave pública del servidor 20.189.173.14? ¿De qué tipo de clave se trata (i.e., para qué algoritmo se utiliza)?

Todas las respuestas irán acompañadas de capturas de pantalla de buena calidad y editadas para resaltar el porqué de la respuesta proporcionada. **En caso de no proporcionar una captura de pantalla como evidencia, la respuesta no será dada por válida.**

EJERCICIO 2: Cortafuegos (3 puntos)

En el Campus Virtual tienes el script `iptables.sh` que se utiliza para la configuración del cortafuegos un determinado equipo que cuenta con tres interfaces de red

- eth0: 192.168.1.2 (a Internet)
- eth1: 192.168.10.1
- eth2: 192.168.3.1

En el script encontrarás 7 líneas que empiezan con el símbolo '#', que sirven para escribir comentarios. Debes **completar de manera clara y concisa estos 7 comentarios** indicando para qué sirven los comandos que aparecen a continuación. La extensión del comentario no debe exceder las dos líneas.

Además, debes responder a las siguientes preguntas argumentando tus respuestas indicando claramente los comandos del script relacionados:

1. ¿Qué servicios pueden ser accedidos desde Internet?
2. ¿Existe una zona desmilitarizada (DMZ) en la red?
3. ¿Los hosts de la red 192.168.10.0/24 pueden acceder a Internet?

4. ¿Pueden los hosts de la red 192.168.10.0/24 recibir conexiones desde Internet?
5. 5. ¿Pueden los hosts de la red 192.168.10.0/24 recibir conexiones desde la red 192.168.3.0/24?

EJERCICIO 3: Certificados y Correo electrónico (3,5 puntos)

En este ejercicio se debe utilizar XCA para crear una autoridad de certificación que emita al alumno un certificado digital para la protección de correo electrónico SMIME. El certificado de usuario deberá contener los datos reales del alumno:

- Nombre y apellidos
- Dirección de email

Utilizando los certificados generados y los proporcionados en el Campus virtual por los profesores de la asignatura enviar un correo electrónico firmado y cifrado a la dirección de correo indicada en el certificado proporcionado por tu profesor de prácticas.

El mensaje a enviar deberá tener la siguiente información:

- **Asunto**: [SMIME 2022-2023] Practica evaluable 2
- **Cuerpo**: Soy <Nombre y Apellidos> del Grupo A/B

ATENCIÓN: Sólo estará permitido el envío de **un único correo** electrónico, que deberá estar **firmado y cifrado**. Si se enviara más de un correo electrónico, sólo se tendrá en cuenta el primero de ellos.