PRÁCTICA 6: Análisis de Protocolos y TLS

Seguridad en la Información

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

EJERCICIO 1 (REPASO): El protocolo TELNET y FTP

En el siguiente enlace de CloudShark[1] hay disponible una captura de tráfico TELNET entre un cliente y un servidor

https://www.cloudshark.org/captures/818ceaef07b8

Esta captura la ha realizado un adversario que se encontraba en la misma red que el cliente, y que busca obtener tanto la información del usuario como los comandos que se han enviado.

Se pide responder a las siguientes preguntas:

1. ¿Cuál es la dirección IP del cliente y cuál es la del servidor?
2. ¿Qué credenciales se han utilizado para acceder al servidor?
    a. PISTA: En esta captura TELNET, el cliente TELNET envía un solo carácter por mensaje en la mayoría de las tramas.
3. ¿Qué tipo de sistema es el servidor?
4. ¿Qué comando(s) ha ejecutado el cliente en el servidor?

El mismo adversario ha capturado también una trama de una comunicación entre un cliente y un servidor FTP

https://www.cloudshark.org/captures/abdc8742488f

Se pide responder a las mismas preguntas que se planteaban para el protocolo anterior. Intenta entender qué ha hecho el cliente.

EJERCICIO 2: El protocolo TLS

En el Campus Virtual tienes a tu disposición un código fuente de Python para crear un servidor HTTPS (HTTP sobre TLS 1.3[2]) en tu equipo. Este servidor utilizará un certificado autofirmado creado en el programa XCA, visto en las prácticas anteriores. Dicho certificado debe estar habilitado para funcionar como servidor TLS/SSL:

- Sujeto: Datos del alumno/a,
- Plantilla: TLS (o SSL) server,
- Uso de la clave con opciones: Digital Signature, Non-Repudiation, Key Encipherment, Key Agreement, y TLS (o SSL) Web Server Authentication,
- Opciones Netscape: SSL Server.

[1] CloudShark es una herramienta de análisis de capturas de tráfico similar a la herramienta de escritorio Wireshark, pero en la nube. De hecho, las capturas se pueden descargar e importar en Wireshark.
[2] En versiones más antiguas de Python (<3.6.15), TLS1.3 no está disponible.

Para lanzar el servidor, es necesario exportar el certificado en formato PEM y la clave privada en formato PEM (no cifrado), y cambiar el código fuente para incluir ambos ficheros.

Ejercicio 2.1. Dado el código fuente con los certificados creados por el alumno/a, capturar la comunicación con el servidor usando Wireshark, y contestar a las siguientes preguntas:

1. ¿Cuándo (de qué trama a qué trama) se procede con el proceso de handshake (sesión SSL), tal y como se ha explicado en teoría?
2. En esta conexión se utiliza TLS1.3. ¿Dónde se negocia exactamente la versión de TLS que se utiliza?
3. En la parte del cliente, ¿en qué trama se puede ver las suites de cifrado que soporta el cliente? ¿Cuáles son?
4. ¿Qué suite de cifrado se acepta finalmente para el proceso de conexión?
5. En TLS1.3, no es posible ver la trama en la que se envía el certificado digital del servidor. ¿Por qué ocurre eso?
    - Adicionalmente, de forma opcional: ¿Sería posible inferir cuál es la trama en la que el servidor envía al cliente su certificado?

Ejercicio 2.2. Cambiar el código fuente para utilizar TLS1.2 en vez de TLS1.3[3]. Contestar entonces a las siguientes preguntas:

1. ¿Cuándo (de qué trama a qué trama) se procede con el proceso de handshake (sesión SSL), tal y como se ha explicado en teoría?
2. En esta conexión se utiliza TLS1.2. ¿Dónde se negocia exactamente la versión de TLS que se utiliza?
3. En la parte del cliente, ¿en qué trama se puede ver las suites de cifrado que soporta el cliente? ¿Cuáles son?
4. ¿Qué suite de cifrado se acepta finalmente para el proceso de conexión?
5. ¿En qué trama se envía el certificado digital del servidor? En esa trama, ¿Dónde se encuentra vuestro nombre (el "common name" cuando creasteis el certificado)? ¿Cuál es la clave pública del servidor?
6. ¿El servidor se autentica al cliente? ¿Y el cliente al servidor?

[3] Ver https://docs.python.org/3/library/ssl.html#constants para encontrar la opción que permite indicar al servidor que deseamos usar explícitamente la versión TLS1.2.

INFORMACIÓN COMPLEMENTARIA

Wireshark / CloudShark

Se aconseja consultar tanto la guía de usuario de Wireshark [1] como la guía de uso de Wireshark de INCIBE [2].

Especificación de protocolos

Los principales RFC [3] referentes a los diferentes protocolos analizados en esta práctica son los siguientes:

- *TELNET*: RFC 854, 855-861
- *FTP*: RFC 959
- *TLS*: RFC 5246, 8446

Referencias:

[1] https://www.wireshark.org/
[2] https://www.incibe-cert.es/seminarios-web/uso-wireshark
[3] https://datatracker.ietf.org/