Tarea 3: Inyectando paquetes UDP en otro socket
Redes
Plazo de entrega: 27 de noviembre 2023

José M. Piquer

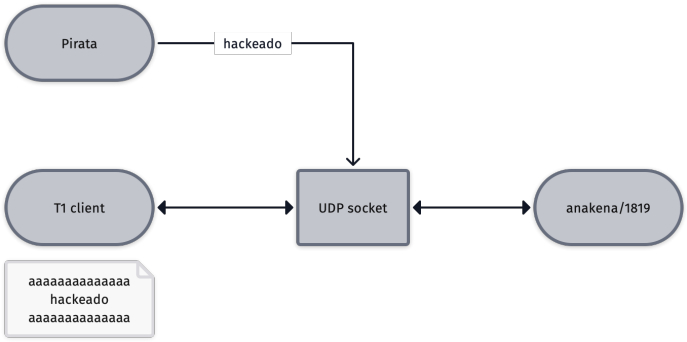

Fig. 1: Esquema general

1. Descripción

Su misión, en esta tarea, es inyectar un mensaje "pirata" en un socket UDP. Usaremos de ejemplo el cliente y servidor de la T1. Con un cliente recibiendo paquetes desde anakena, Uds deben generar desde otro proceso, en el mismo computador del cliente, un paquete UDP que le llegue al cliente y este lo interprete como un paquete de datos desde el servidor y lo escriba erróneamente en el archivo de salida. Para eso, el paquete que Uds envían debe estar construido de tal forma que venga con los headers IP y UDP modificados para que parezca ser un paquetes de datos desde anakena.

Para esto se les pide usar *scapy*, un sistema para manipular a mano paquetes de red. Uds deben "falsificar" un paquete UDP para que el cliente crea que viene del servidor y así lo responda. Scapy se puede usar directamente con un script o pueden usar el módulo para Python que permite utilizarlo desde dentro de un programa.

Para lograr que el paquete le llegue al cliente existente, necesitamos una información extra: el número de puerto UDP que el cliente está usando en su extremo. El del servidor lo conocemos, es el 1819 de siempre. Pero el del cliente es aleatorio y cambia para cada cliente. Para esto, deben agregar la siguiente línea al cliente de la T1:

```
print(s.getsockname())
```

.

Así el cliente escribe en su salida el número de puerto asignado. Una versión de ese servidor sigue corriendo en anakena en el puerto 1819 para que lo usen en sus pruebas.

Además de ingresar al socket UDP, el paquete inyectado debe respetar el protocolo de la T1, de modo que el cliente crea que ese es el paquete que le corresponde. Para esto, deben adivinar el número de secuencia que está esperando el cliente. Por esto, se sugiere hacer un pirata que intente miles de veces inyectar un paquete 'D' con un número de secuencia que vaya iterando secuencialmente entre 00 y 99. De esta forma, si logran entrar con un número de secuencia correcto, pueden lograr varios paquetes 'hackeados' seguidos puesto que todos irán en orden. Recuerden que el pirata no puede recibir respuestas, por lo que nunca recibirá un ACK. El ataque tienen que hacerlo a ciegas.

HINTS:

- Windows: Además de instalar scapy, deben instalar npcap
- Linux: para poder probar en 127.0.0.1, deben agregar la línea:

  ```
  conf.L3socket=L3RawSocket
  ```

- MacOSX: Todo funciona, pero no agreguen la línea anterior, que hace que nada más funcione!

2. Ejecución

En un terminal ejecuten el cliente de la T1 y lo dejan corriendo (tiene que ser un archivo grande y con paquetes chicos para que demore su ejecución). En otro terminal (en el mismo computador que el cliente) corren el pirata como:

```
% ./pirata.py anakena.dcc.uchile.cl 1819 XX.XX.XX.XX NNNN
```

En XX.XX.XX.XX ponen su dirección IP actual y en NNNN el número de puerto que está usando el cliente. Los paquetes IP que el programa pirata inyecta van con origen anakena/1819 y destino XX.XX.XX.XX/NNNN para que el socket UDP los acepte.

3. Entregables

Básicamente entregar el archivo con el pirata que logra el objetivo y un archivo que explique cómo usarlo para inyectar paquetes erróneos al cliente de la T1. Deben lograr que el cliente normal de la T1 reciba de vuelta del server al menos una línea que diga "hackeado" y se escriba en el archivo de salida. Explique en detalle el sistema operativo y el ambiente en que probó la tarea para poder replicarlo.

En un archivo aparte responder las preguntas siguientes (digamos, unos 5.000 caracteres máximo por pregunta):

1. Si usara este mismo pirata para la T2: ¿funcionará inyectar un paquete? ¿Será más fácil o más difícil?.

2. Este ejercicio muestra lo trivial que es la seguridad en UDP. Si uno quisiera tener un sistema seguro en UDP, ¿cómo podríamos protegernos de este tipo de falsificaciones?

3. En TCP, ¿sería igual de trivial inyectar un paquete de datos?

4. Si ahora queremos que el pirata esté en otro computador que el cliente, ¿se podría hacer lo mismo con scapy? ¿Cómo?

5. Revise el tanaño del archivo de salida una vez que logró inyectar al menos un paquete pirata. ¿es más grande o más chico? Explique por qué.