Parte 1

Cuestión 1(1 punto)

Explique las diferencias entre exploit y payload, para qué se utiliza cada uno y qué relación tienen entre sí.

Un exploit, es un programa que se encarga de aprovechar una vulnerabilidad en un sistema, atacándolo para obtener información sensible, o cualquier tipo de acción maligna que quiera realizar el atacante. El payload viene a ser , el fragmento de codigo que hace el daño. Para un mejor entendimiento de esto, imaginemonos un misíl nuclear. Tenemos el cohete, que vendría a ser el exploit. El cohete es el motor que dirige el misíl, y sin el, es imposible transportar la ojiva. La ojiva es lo que realmente hace el daño, es por esto que lo podríamos comparar con el payload.

Cuestión 2(1 punto)

Escriba al lado de cada tipo de función si se trata de una función de tipo simétrico, de tipo asimétrico, un algoritmo de hashing o una función de codificación.

MD5: Algoritmo de hashing

SHA1: Algoritmo de hashing

BASE64: Algoritmo de codificación

AES: Función de tipo simétrico

RSA: Función de tipo asimétrico

Cuestión 3(1 punto)

Se desean conectar dos redes de forma que se puedan realizar comunicaciones desde todos los equipos de una LAN hacia los equipos de otra a través de un tunel. Los equipos deben de poder ser directamente accesibles, de manera que si hacemos un ping, un ssh o cualquier tipo de comunicación podamos enviar los paquetes a la IP destino. ¿Cuales de estos programas nos permiten hacer esto sin necesidad de combinarlos con otros? Se supone que configuraremos las rutas de los hosts de forma correcta.

Iptables, ettercap, ppp, ssh -r ...,ssh -l …, socat, openvpn

ssh -R, ssh -L --> Esto son comandos que necesitaremos usar
En cuanto a los programas --> Openvpn,socat

Cuestión 4(1 punto)

Tenemos un ordenador con servidor ssh habilitado. La ruta del archivo de configuración del sshd es */etc/sshd/sshd_conf*. Hemos generado un usuario llamado luis con home en */home/luis*. Y tenemos en un USB conectado al ordenador los archivos *luis* y *luis.pub* que contienen la clave privada y publica respectivamente. Deseamos poder acceder sin necesidad de introducir la password a ese ordenador mediante el usuario *luis* utilizando el par de claves descritas del USB. ¿Que cambios mínimos deberemos de realizar para conseguirlo? (sea conciso)

Copiamos la clave publica con el comando 'ssh-copy-id' al servidor de ssh

> ssh-copy-id ssi29@192.168.56.102

> ssi29 #use the password

Una vez copiado, ahora somos capaces de conectarnos al servidor sin que nos pida contraseña

> ssh ssi29@192.168.56.102

AllowUsers <Usuario>

Cuestión 5(1 punto)

Cuando intentamos acceder a la web websecreta.ibm.com nos pide autenticación web para poder verla. Esnifando en la wifi de la empresa hemos obtenido el siguiente paquete:

```
20:02:10.605822 IP madremia.unavarra.es.54611 > websecreta.ibm.com.http: Flags [.], ack 13033, win
432, options [nop,nop,TS val 178301668 ecr 3533092013], length 0

GET /index.html HTTP/1.1

Host: websecreta.ibm.com

Authorization: Basic bGFsYWxhOmxvbG9s
```

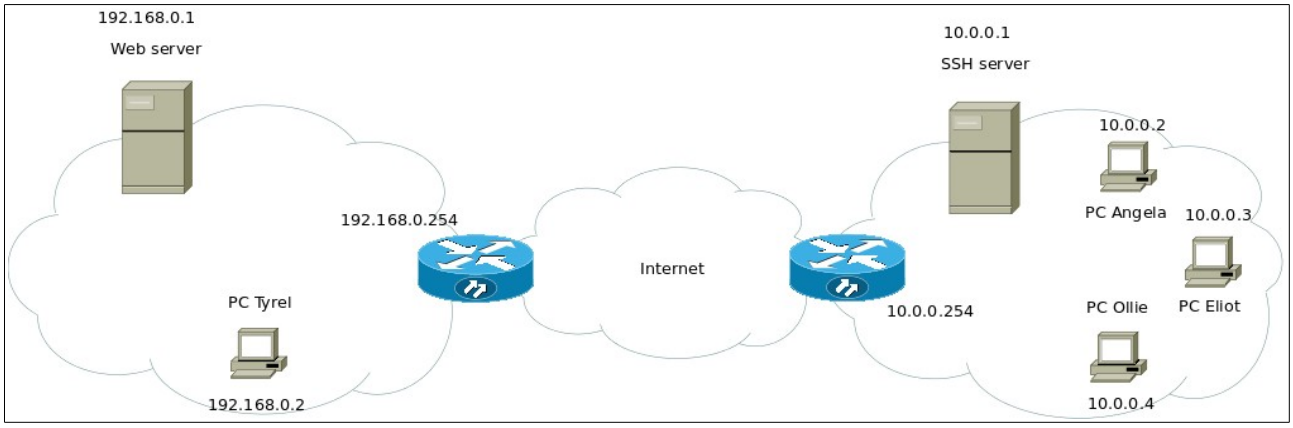
¿Existe alguna forma de que podamos acceder a dicha web sin realizar ningún ataque de MITM? ¿Como?

openssl enc -d -base64 "bGFsYWxhOmxvbG9s"

Parte 2

Escenario 1(2.5 puntos)

Tenemos un escenario en el que hay un trabajador llamado Tyler que está trabajando desde casa para una empresa. El escenario es el que viene descrito por la imagen siguiente:



En su casa dispone de un servidor web en el que tiene el sistema de pruebas (funcionando en el puerto 80). Tyler tiene serias sospechas de que Elliot puede ser un hacker a pesar de ser personal de la empresa por lo que desea que desde su pc (el de Elliot) no tenga acceso al servidor Web pero tiene que dejar acceso a Angela y Ollie para que puedan acceder a él y que prueben el sistema. El primer problema que tiene es que no tiene acceso a su propio router ya que si cambia la password o cualquier configuración del router su proveedor de telefonía le corta la conexión.

El router de Tyrel hace NAT de sus máquinas interiores las cuales tienen todas IPs de rango local (192.168.0.X). Supondremos que las direcciones IP de la empresa son todas de rango global (A pesar de que por simplificar se ha usado el espacio de direcciones 10.0.0.x) por lo que desde la red interna de Tyrel puede acceder a las direcciones IP de la empresa (La configuración es muy similar a las que tenemos casi todos en casa).

Tyrel tiene un usuario (con privilegios de root) en el servidor de ssh y ejecuta el siguiente comando desde su pc con la intención de que los ordenadores de su empresa puedan acceder a su servidor Web interno:

```
ssh tyrel@10.0.0.1 -L 80:192.168.0.1:6000     ssh -R 6000:192.168.0.1 tyler@10.0.0.1
```

La intención de Tyrel es que los miembros de la empresa se conecten a la dirección IP 10.0.0.1 al puerto 6000 y que tengan acceso al servidor Web de pruebas. Además, como Tyrel no se fía de Eliot desea que a su servidor no tenga acceso la dirección IP de Eliot. Así que se mueve a la habitación donde tiene el servidor y ejecuta las siguientes sentencias en la terminal de root de su servidor web:

```
iptables -P INPUT DROP
iptables -A INPUT -src 10.0.0.2 --dst-port 80 -j ACCEPT
iptables -A INPUT -src 10.0.0.4 --dst-port 80 -j ACCEPT
iptables -A INPUT -src 192.168.0.2 --dst-port 80 -j ACCEPT
iptables -A INPUT -src 192.168.0.2 --dst-port 22 -j ACCEPT
```

Correcto
Cambiar todos los siguientes a FORWARD

OJO! El firewall lo vamos a colocar en el servidor ssh antes de crear el tunel, porque este no conoce el origen ni el destino

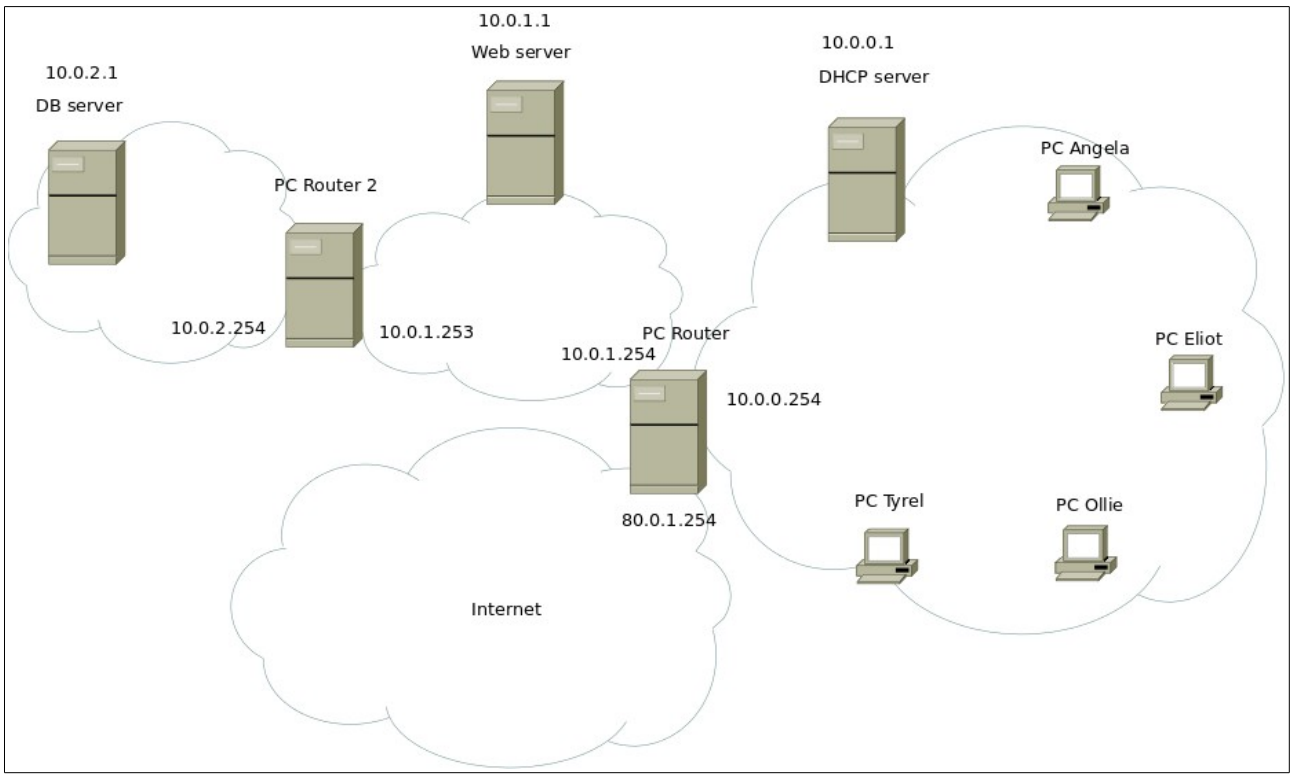
Aparte de las direcciones IP de Angela y Ollie su intención es permitir el acceso a su ordenador de casa para poder acceder al menos a los puertos 22 (para subir sus programas) y Web (para verificarlos).

¿Es correcta la configuración realizada por Tyler? Diga que partes están mal realizadas y por qué en caso de que estén mal y que cambios debería realizar Tyler y en qué ordenadores para permitir el acceso. Recuerde que Tyler solo tiene control root sobre su servidor Web, su PC y mediante ssh sobre el servidor ssh. Tenga en cuenta que Elliot no debería poder acceder al servidor Web de Tyler pero debería poder trabajar en sus proyectos en la empresa.

En caso de que la configuración de Tyler esté bien realiza, describa claramente como se realiza la conexión, por parte de Ollie, al servidor web de Tyler. Que debe poner en el navegador, que partes de la comunicación van cifradas y cuales no, y en que parte se esta cortando el acceso al ordenador de Elliot (desde donde hasta donde puede acceder Elliot y donde se cortan los paquetes enviados por Elliot).

Escenario 2(2.5 puntos)

Tenemos el escenario siguiente:



En la empresa que refleja vemos los ordenadores de sus únicos 3 trabajadores, Tyrel, Angela y Ollie y además hay un hacker llamado Elliot que ha conseguido pinchar su ordenador dentro de los switches de la empresa con un cable largo, a través de una ventana. El hacker se encuentra fuera del edificio pero con un ordenador con conexión vía cable a los switches de la empresa.

La empresa abre a las 8:00 de la mañana, hora en que los trabajadores encenderán sus ordenadores que tienen configurada la dirección IP de forma dinámica mediante DHCP. Además tiene protección MAC con lo que sólo ofrecerá dirección IP a las MAC del ordenador de Tyrel, de Angela y de Ollie. Su pool de direcciones IP es de la 10.0.0.10 a la 10.0.0.12 y el router por defecto que pone es el 10.0.0.254.

Dicho router es un pc configurado con un IP tables que solo permitirá en su cadena de INPUT en la interfaz perteneciente a la 10.0.0.x la entrada sólo a paquetes con alguna de las tres MACs descritas anteriormente.

Angela y Ollie son trabajadores que se dedican a meter datos en la base de datos a través de la pagina Web del servidor 10.0.1.1 y Ollie está enfermo y no ha podido ir a trabajar (por lo que su ordenador no se encenderá). Los trabajadores meten tantos datos y de forma tan persistente que un ordenador común (como el de Elliot) no podría enrutar todo el tráfico que generan y se dedican toda su jornada laboral a meter datos personales de clientes. Tyler es el jefe y se dedica a navegar por Internet y buscar productos con precios módicos y a twitear.

El servidor Web 10.0.1.1 tiene configuradas 3 reglas en la cadena INPUT que permiten sólo la recepción de paquetes desde 3 direcciones IP, la 10.0.0.10, la 10.0.0.11, la 10.0.0.12 y la 10.0.2.1. El resto de paquetes los tira.

El Servidor de bases de datos 10.0.2.1 tiene una regla de iptables en la cadena INPUT que permite solo la recepción de paquetes desde la dirección IP 10.0.1.1.

El php que permite introducir datos en la base de datos del servidor web es el siguiente:

```
<?php


mysql_connect(10.0.2.1,”root”,”patata”);


$SQL=”SELECT * FROM Clientes WHERE DNI=”.$_GET['DNI'];
$RES=mysql_query($SQL);
if(0==mysql_num_rows($RES)){
	$SQL=”INSERT INTO Clientes VALUES (NULL,”.$_GET['DNI'].”,”.$_GET['CUENTA_BANCARIA'].”)”;
	mysql_query($SQL);
}else{
	$SQL=”UPDATE Clientes SET Numero_cuenta=”.$_GET['CUENTA_BANCARIA'];
	mysql_query($SQL);
}


?>
```

Y la pagina web (llamada inserta.php) está en la carpeta /var/www/, donde el usuario www-data, que es el que corre el servidor apache, tiene privilegios de escritura.

No existen más paginas web que la del formulario de entrada que enlaza con esta pagina php, que se llama fomulario.html.

A Eliot se le ha encargado la siguiente misión, obtener todos los datos introducidos en la base de datos. Es importante que los trabajadores de la empresa puedan realizar su trabajo de forma normal. Eliot dispone de toda la información que se da en este ejercicio ademas de las MACs de los tres ordenadores de los trabajadores, del router y del servidor de DHCP.

¿Que pasos debe de hacer Eliot y con que objetivo para obtener los datos requeridos? Marcar cada paso que se deséa hacer con el comando que ejecutaría o dato de entrada específico que metería y que se consigue con cada uno.

1. Mac spoofing con la mac de ollie
2. DHCP para obtener una IP valida

Opcion 1. Conectarse por ssh al servidor web. TUNNELING y de ahí ejecutar comandos para coger toda la info

Opcion 2. SQL injection haciendo que el servidor sql pueda se pueda acceder desde mas ips

De esta forma desde la ip de elliot podremos acceder al servidor de base de datos.

(En el caso de que usuario root patata tenga permisos de modificar ips de acceso). Una vez que tenga permisos puede conectarse al servidor web con las credenciales del php (en el caso de que las sepa root y patata).

Opcion 2.2. Sin embargo en el caso de que no sepa las credenciales. Podemos realizar otro SQL injection en el que añadamos un nuevo usuario a la base de datos y así poder tener credenciales para acceder a la base de datos desde el ordenador de elliot.

OBJETIVO COMPLETADO

Una vez hemos realizado el ataque y haber cogido toda la información requerida es hora de cubrir las huellas y que no se den cuenta de lo ocurrido.

Una vez ya tenemos acceso a la base de datos eliminamos nuestro usuario creado y cambiamos los permisos de ip con SQL injection sobre la pagina web. Una vez realizado esto no nos queda nada mas, hemos dejado todo como estaba.