AUDITORIA METASPLOITABLE 2

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

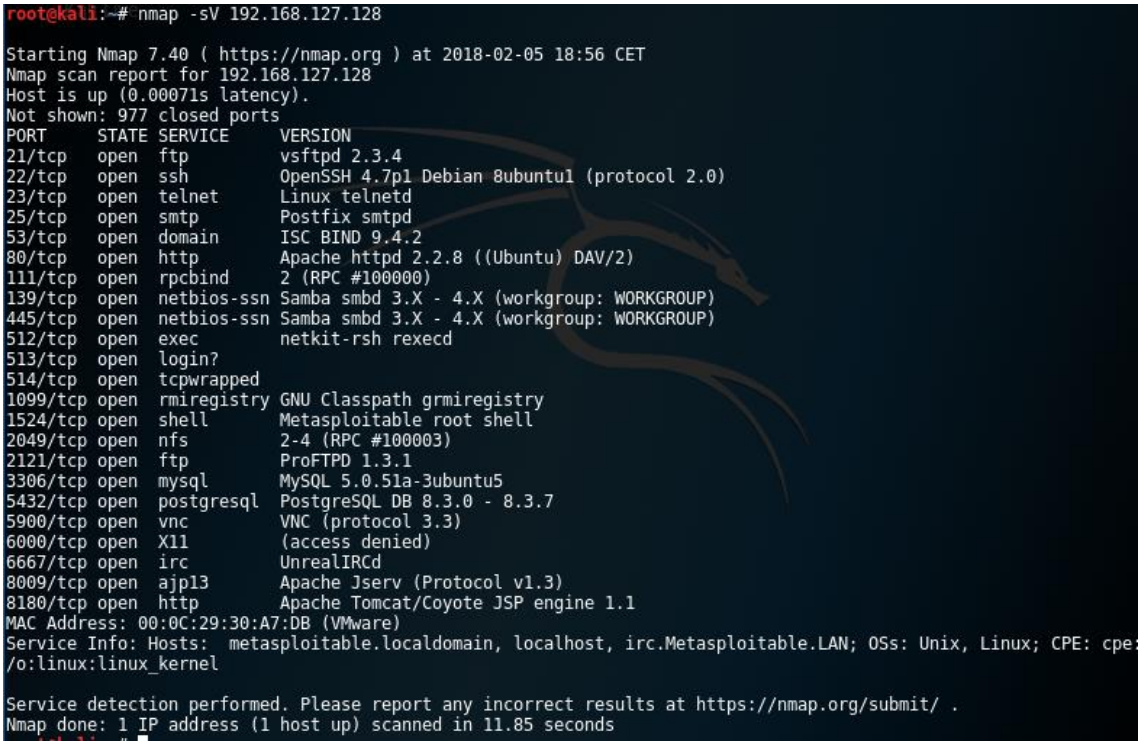
Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

Rafael Osuna Ventura
2ºASIR

El objetivo de esta auditoría es explotar los diferentes servicios de la máquina Metasploitable 2. Para ello sabemos su dirección IP: 192.168.127.128.

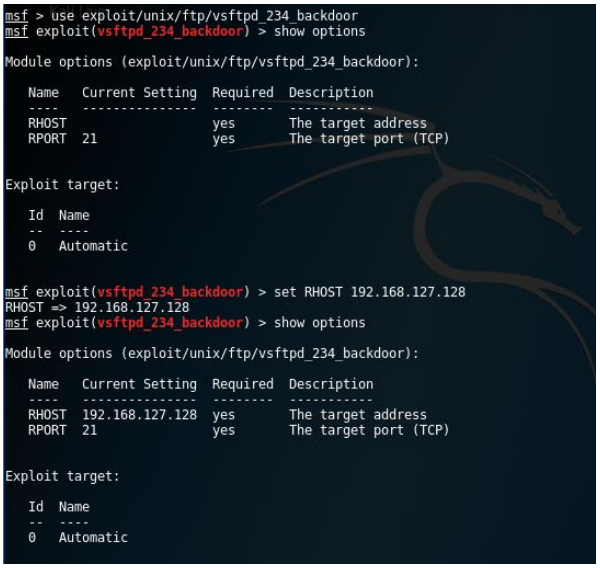
Si realizamos un escaneo de puertos usando el comando ***"nmap –sV dirección IP de la víctima"*** , nos aparecen todos los puertos que están abiertos y los servicios correspondientes a dichos puertos, estos serán los que intentemos atacar.

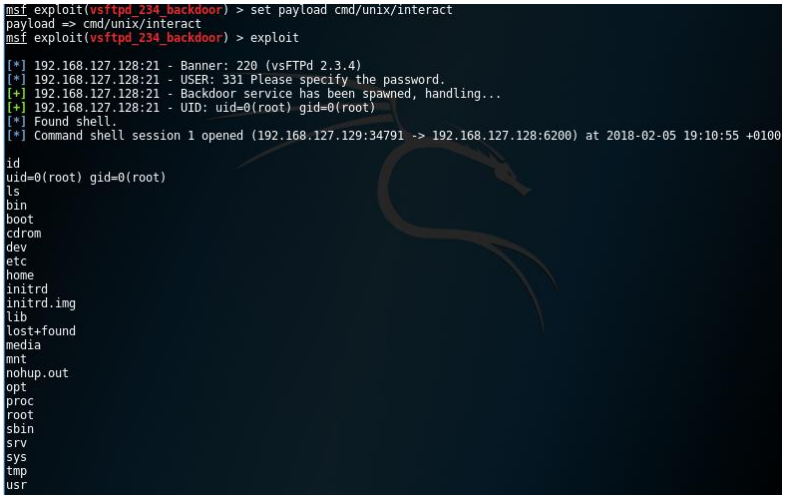


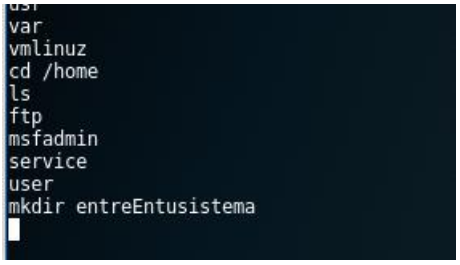
Rafael Osuna Ventura
2ºASIR

EXPLOTACIÓN DE VULNERABILIDADES

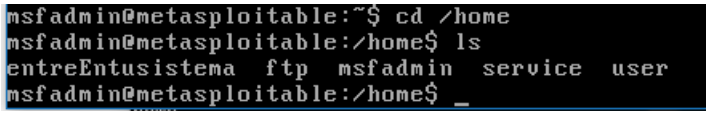
1.- Se trata del servicio ftp en su versión vsftpd 2.3.4, es una puerta trasera que permite el acceso remoto a la maquina víctima. Usaremos el exploit: exploit/unix/ftp/vsftpd_234_backdoor.





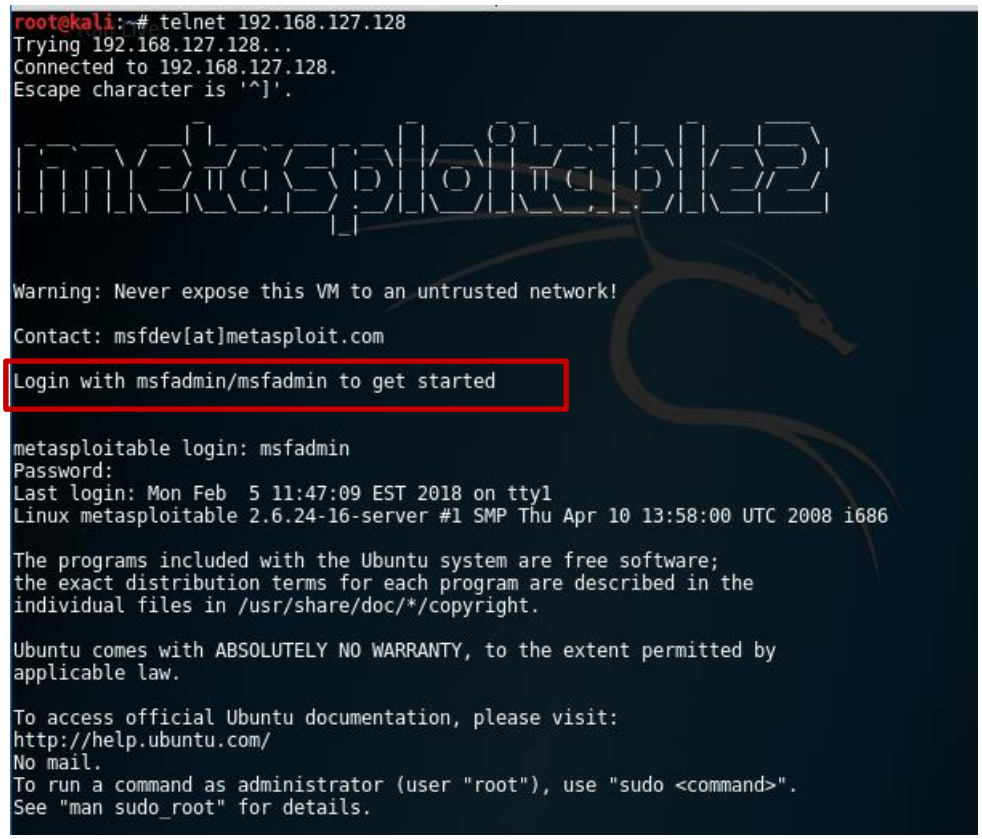


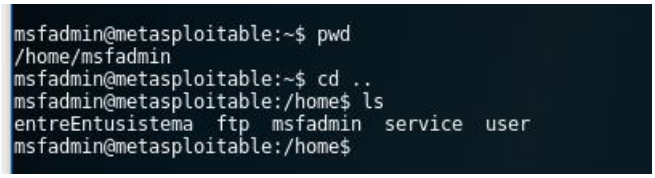
Al realizar esto estaríamos creando un fichero en su máquina:



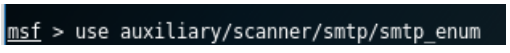
Rafael Osuna Ventura
2ºASIR

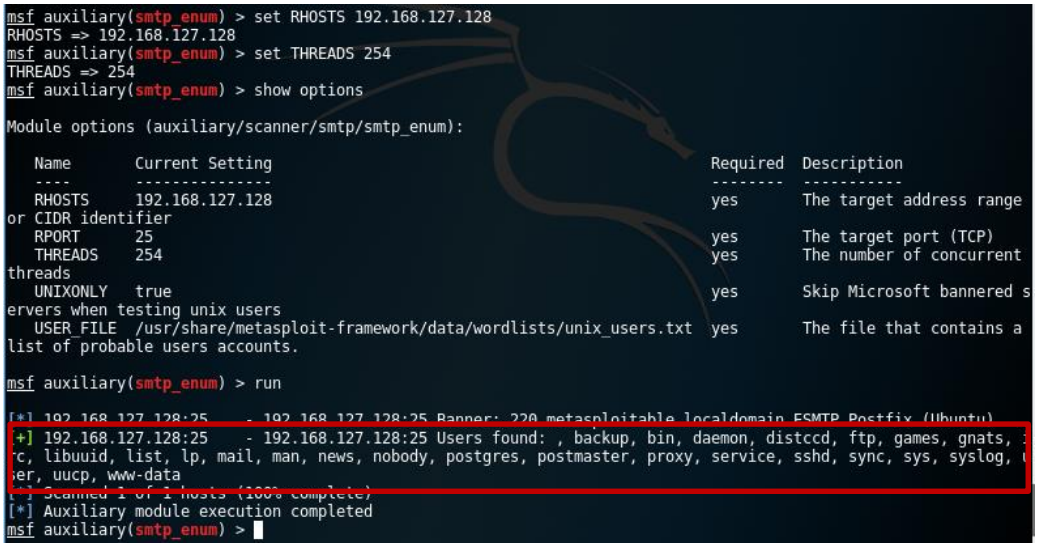
2.- Servicio telnet en su versión Linux telnetd. Al intentar conectarnos mediante telnet, este nos da el usurio y contraseña pudiendo acceder así a la maquina victima.



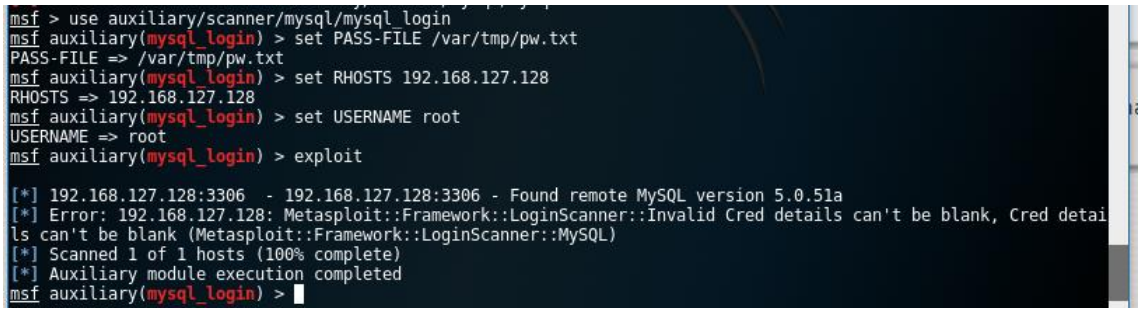


3.-Servicio smtp en su versión Postfix smtpd. Nos muestra todos los usuarios que tiene el sistema usando el exploit:

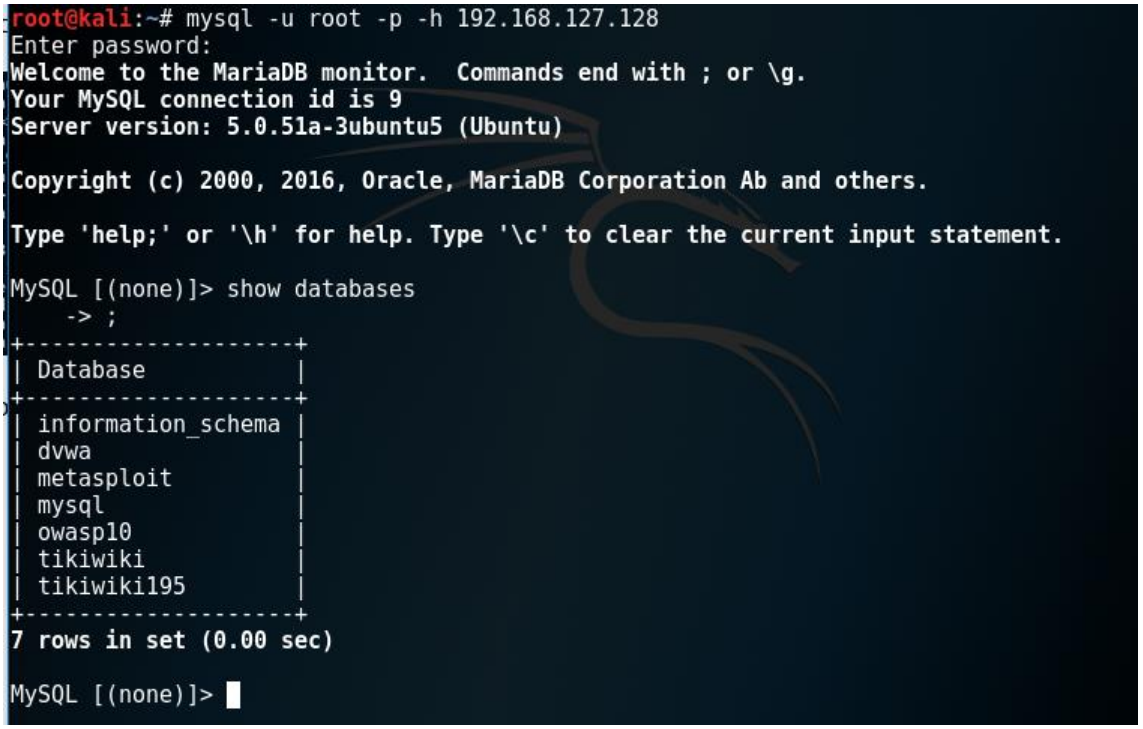




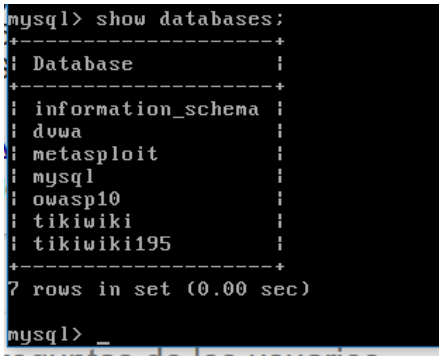
4.- Servicio mysql en su versión MYSQL 5.0.51, este creará una puerta trasera para ejecutar comando. Usaremos el exploit: auxiliary/mysql/mysql_login. Este no nos da resultado.



Probamos a acceder con el comando “mysql –u root – p –h dirección ip de la víctima”:

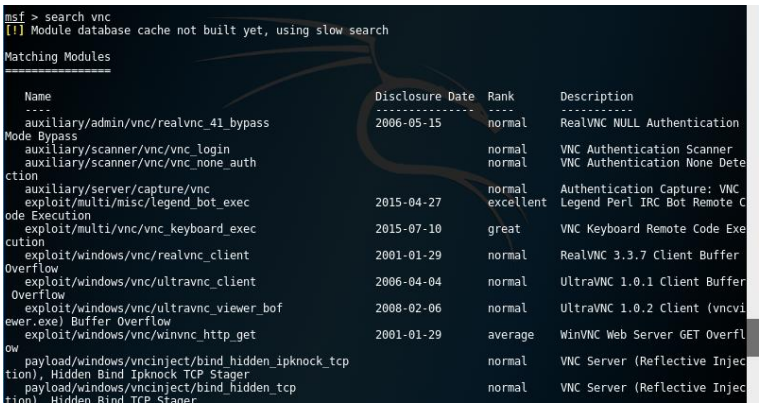


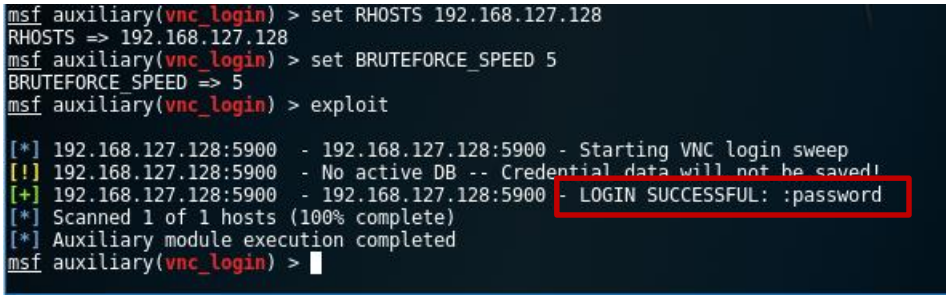
Como vemos podemos administrar las bases de datos que nos aparecen en la maquina vicitma.



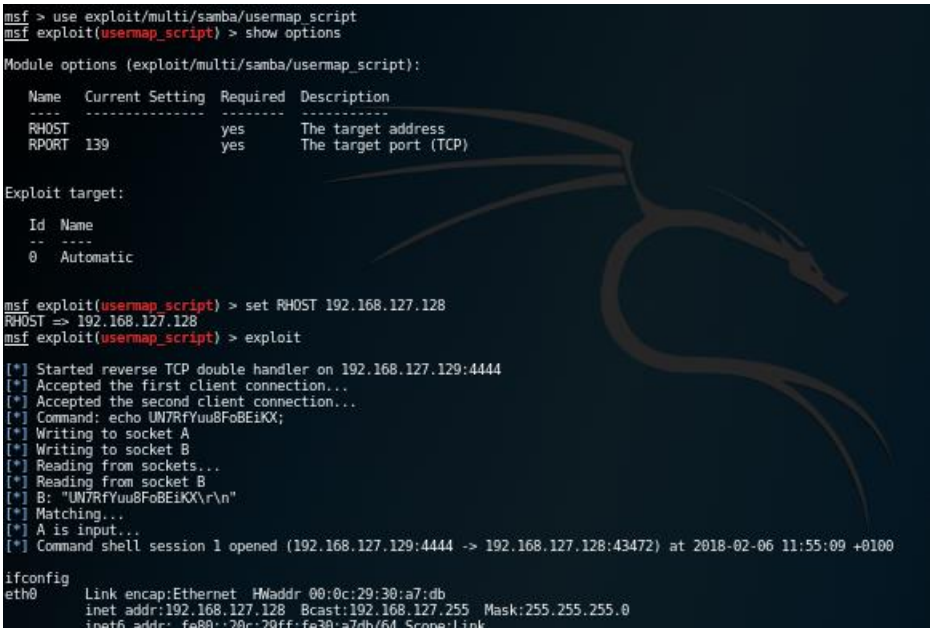
Rafael Osuna Ventura
2ºASIR

5.- Servicio vnc en su versión VNC (protocol 3.3).Obtenemos la contraseña de lservidor VNC.Usaremos el exploit: auxiliary/scanner/vnc/vnc_login



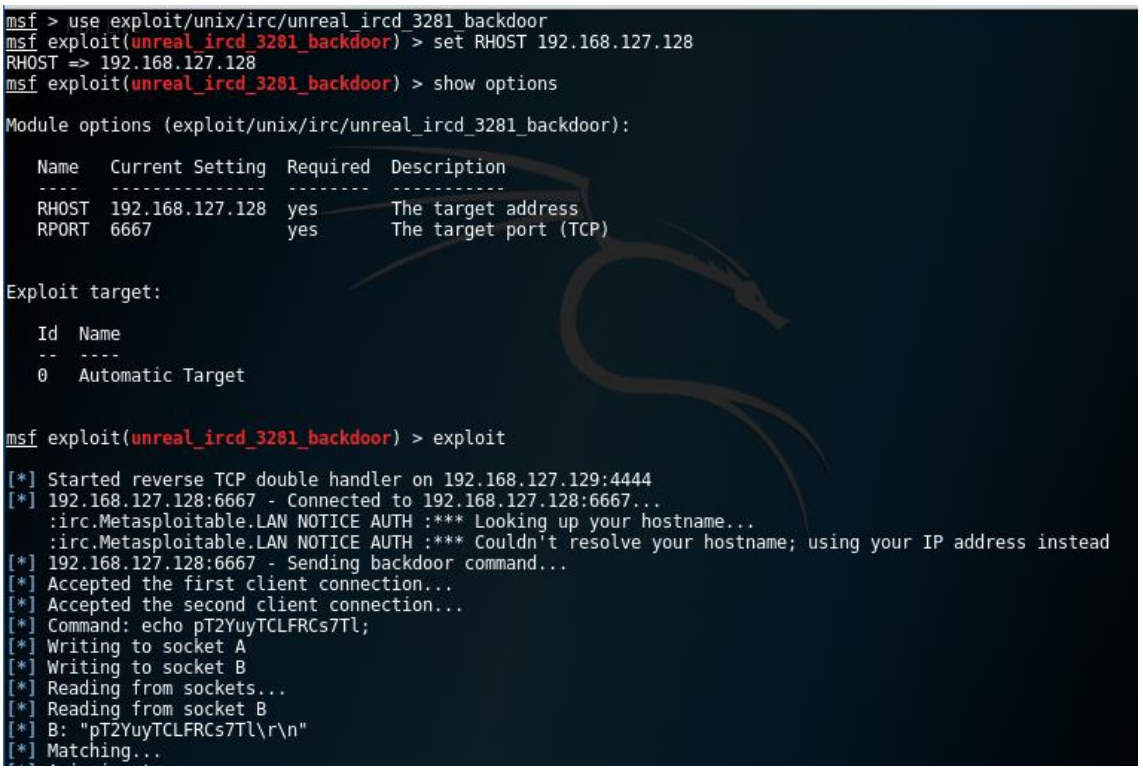


6.- Servicio ajp13 en su versión Jserv v1.3. Permite ejecutar comandos. Usaremos el exploit: exploit/multi/samba/usermap_script

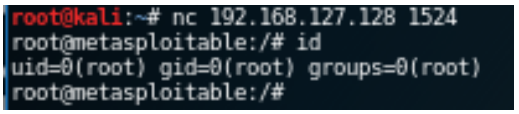


Rafael Osuna Ventura
2ºASIR

7.-Servicio irc en su versión unreal ircd. Creará una puerta trasera para la ejecución de comandos. Usaremos el exploit: exploit/unix/irc/unreal_ircd_3281_backdoor



8.- Servicio Shell en su versión Netkit rshd. Obtención de datos al conectarnos con la víctima. Usaremos el comando “nc ipcíctima puerto”



COSAS A CAMBIAR

- Servicios mal configurados: muchos servicios dan acceso al sistema operativo
- Puertas traseras: se pueden usar para obtener acceso al sistema operativo.
- Contraseñas débiles: son vulnerables a ataques de fuerza bruta.