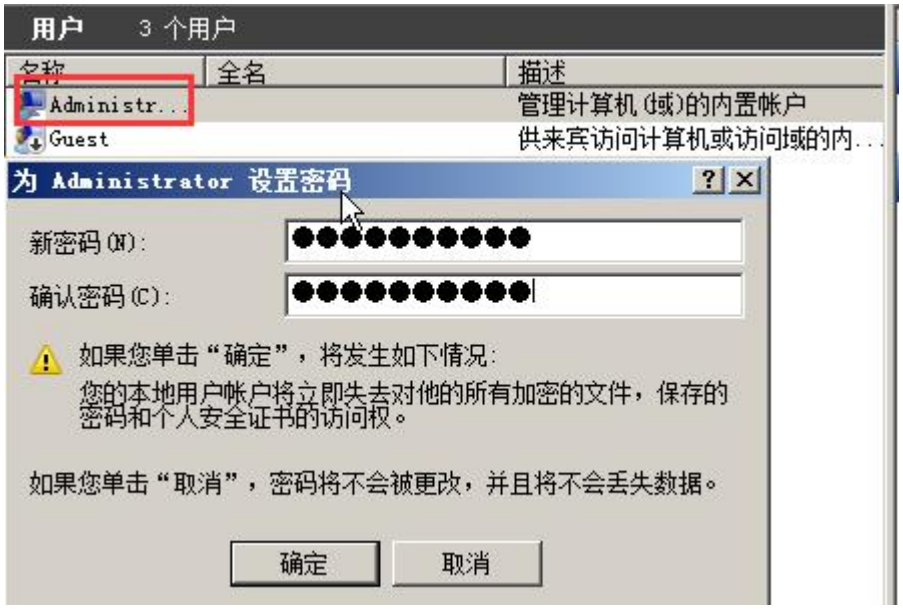
Windows 靶机加固（5 个得分点）

1. 删除后门用户，若在命令行下操作也正确（15 分）

若无漏洞发现过程或思路扣 5 分

2. 为管理员用户设置较为复杂的密码，若在命令行下操作也正确（15 分



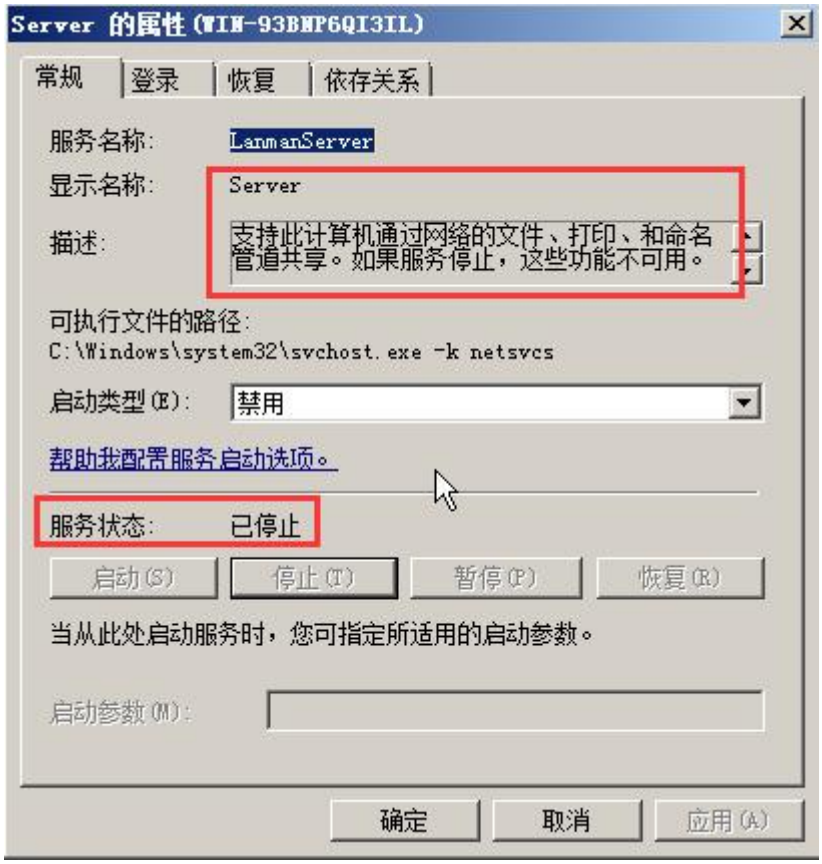
3. 禁用 IIS 内核缓存，避免对方利用 ms15_034 漏洞进行 DOS 攻击，

去掉【启用内核缓存】复选框前面的钩（25 分）

若无漏洞发现过程或思路扣 5 分

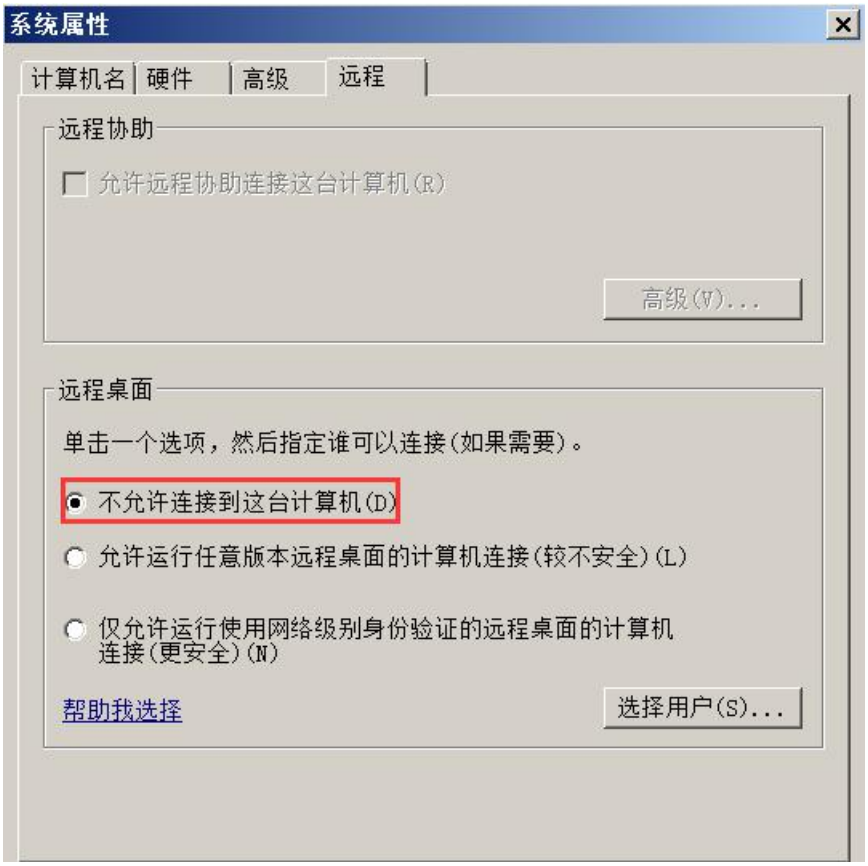
若无漏洞验证过程扣 10 分

4. 防范 ms17_010 等漏洞进行攻击，停止 Server 服务。（25 分）



若无漏洞发现过程或思路扣 5 分
若无漏洞验证过程扣 10 分

5.避免对方利用 ms12_020 漏洞进行 DOS 攻击而出现蓝屏现象，关闭远程桌面服务。（20 分）



若无漏洞发现过程或思路扣 5 分
若无漏洞验证过程扣 10 分

Linux 靶机加固（7 个得分点）

1.找到异常用户，使用命令“userdel”进行用户删除操作，修改这两个用户的密码也可以（5 分）

```
[root@test ~]# userdel drgsup836
userdel: group drgsup836 not removed because it is not the primary group of user dr
gsup836.
[root@test ~]# userdel amercn416
userdel: group amercn416 not removed because it is not the primary group of user am
ercn416.
```

若无漏洞发现过程或思路扣 3 分

2. 修改 root 用户的密码（6 分）

```
[root@test ~]# passwd
Changing password for user root.
New password:
BAD PASSWORD: it does not contain enough DIFFERENT characters
BAD PASSWORD: is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@test ~]#
```

3. 禁止 root 用户通过 SSH 服务登录服务器（7 分）

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

若无漏洞发现过程或思路扣 2 分

若无漏洞验证过程扣 3 分

4. VSFTPD2.3.4，因为需要服务正常运行，通过火墙添加固。（25 分）

```
[root@test Desktop]# iptables -A INPUT -m state --state NEW -m tcp -p t
cp --dport 6200 -j DROP
```

若无漏洞发现过程或思路扣 5 分

若无漏洞验证过程扣 10 分

5. 修改数据库用户 root 的密码，避免对方以过弱口令暴力破解的方式登录数据库，（18 分）

```
mysql> update user set authentication_string=password('p@ssw0rd1!') where user='root';
Query OK, 0 rows affected, 1 warning (0.00 sec)
Rows matched: 3  Changed: 0  Warnings: 1

mysql>
```

若无漏洞发现过程或思路扣 5 分

6. 禁止数据库用户 root 从任意地点登录（17 分）

```
mysql> delete from user where host='%' and user='root';
Query OK, 1 row affected (0.00 sec)

mysql>
```

或

```
mysql> drop user 'root'@'%';
Query OK, 0 rows affected (0.00 sec)
```

等，（只要是禁止 root 用户从任意地点登录都为正确）

若无漏洞验证过程扣 10 分

7. 后门程序删除（22 分）

```
[root@test ~]# rm -rf cpufan
[root@test ~]#
```

若无漏洞发现过程或思路扣 10 分

若无漏洞验证过程扣 10 分