2021全国职业技能大赛-网络安全赛题解析总结②（超详细）

原创

落寞的鱼丶 于 2021-10-28 10:29:38 发布 6259 收藏 30

分类专栏： 2021全国职业技能大赛-网络安全赛题解析 文章标签： web安全 linux 安全

本文链接：https://blog.csdn.net/Aluxian_/article/details/120985302

2021全国职业技能大赛-网络安全赛题解析总结（2）

模块A 基础设施设置与安全加固

有问题可以私信博主哦~

模块A 基础设施设置与安全加固

一、项目和任务描述：

假定你是某企业的网络安全工程师，对于企业的服务器系统，根据任务要求确保各服务正常运行，并通过综合运用登录和密码策略、数据库安全策略、流量完整性保护策略、事件监控策略、防火墙策略等多种安全策略来提升服务器系统的网络安全防御能力。本模块要求对具体任务的操作截图并加以相应的文字说明,以word文档的形式书写,以PDF格式保存,以赛位号作为文件名。

二、服务器环境说明：

Windows 用户名：administrator，密码：123456

Linux 用户名：root，密码：123456

A-1任务一 登录安全加固（Windows, Linux）

请对服务器Windows、Linux按要求进行相应的设置，提高服务器的安全性。

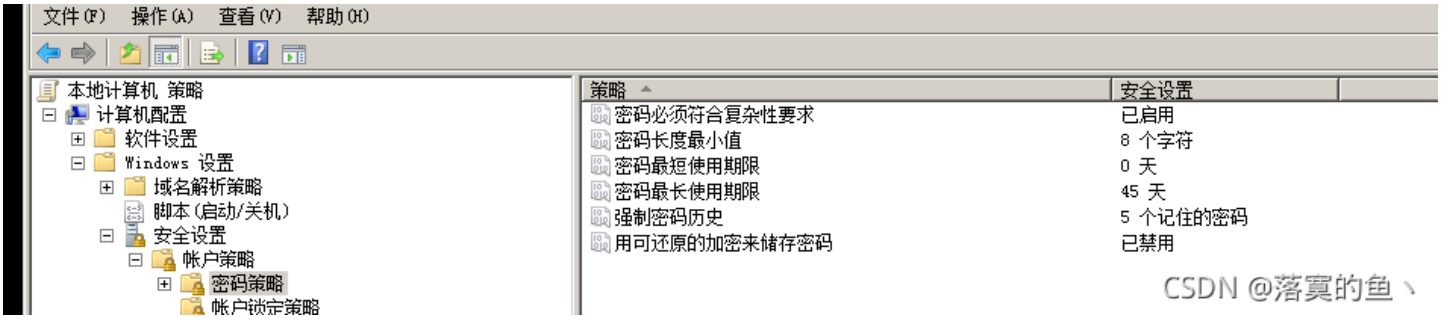
1.密码策略（Windows, Linux）

a.强制密码历史为5个密码；

b.密码最长存留期为45天。

> windows：Win + R gpedit.msc 打开本地组策略编辑器

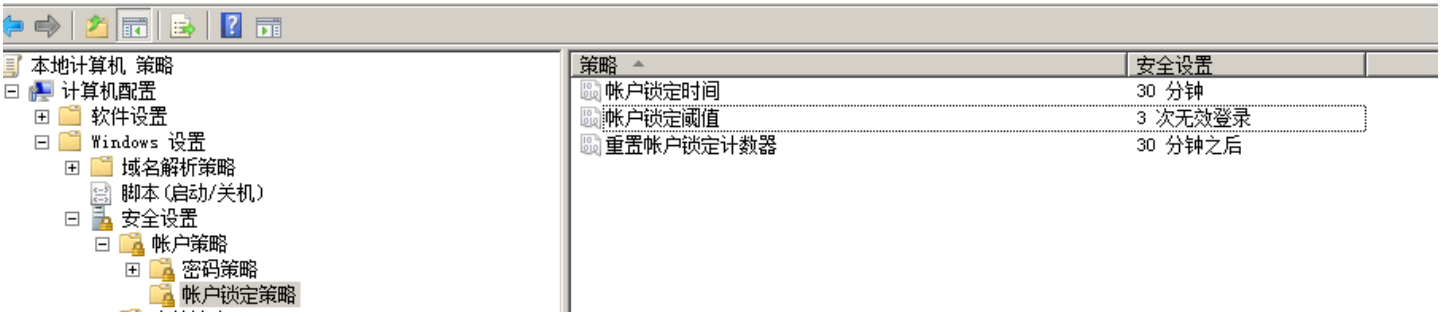
Windows：管理工具-本地安全策略-帐户策略-密码策略，设置密码厉害为5个，保留天数为45天。



2.登录策略（Windows）

a.设置账户锁定阈值为3次错误锁定账户，锁定时间为30分钟，复位账户锁定计数器为30分钟之后。

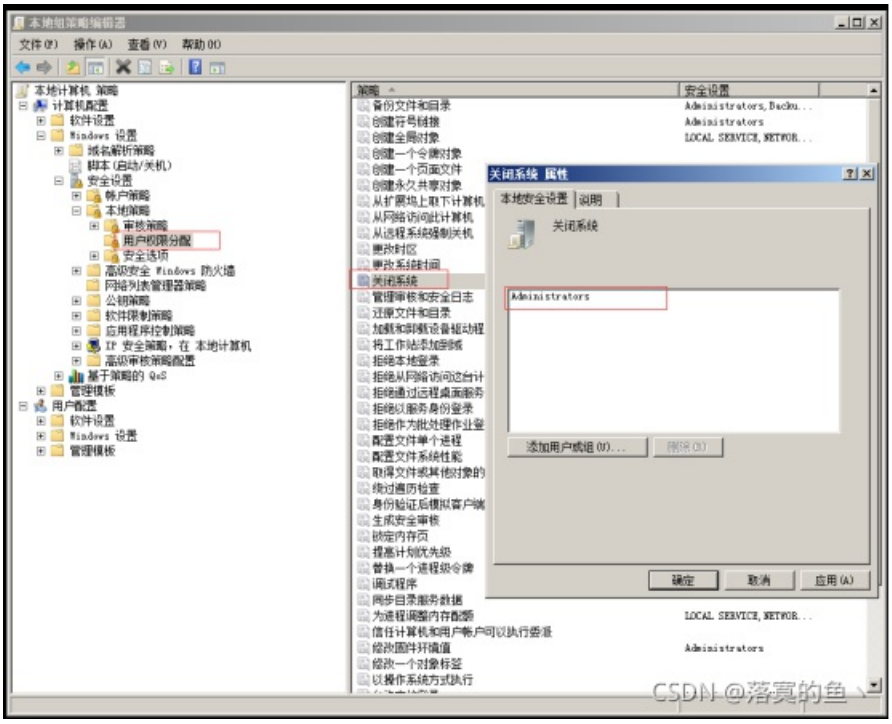
Windows：管理工具-本地安全策略-帐户策略-账户锁定策略，设置锁定时间30分钟，锁定阈值为3次，锁定计数器为30分钟之后。



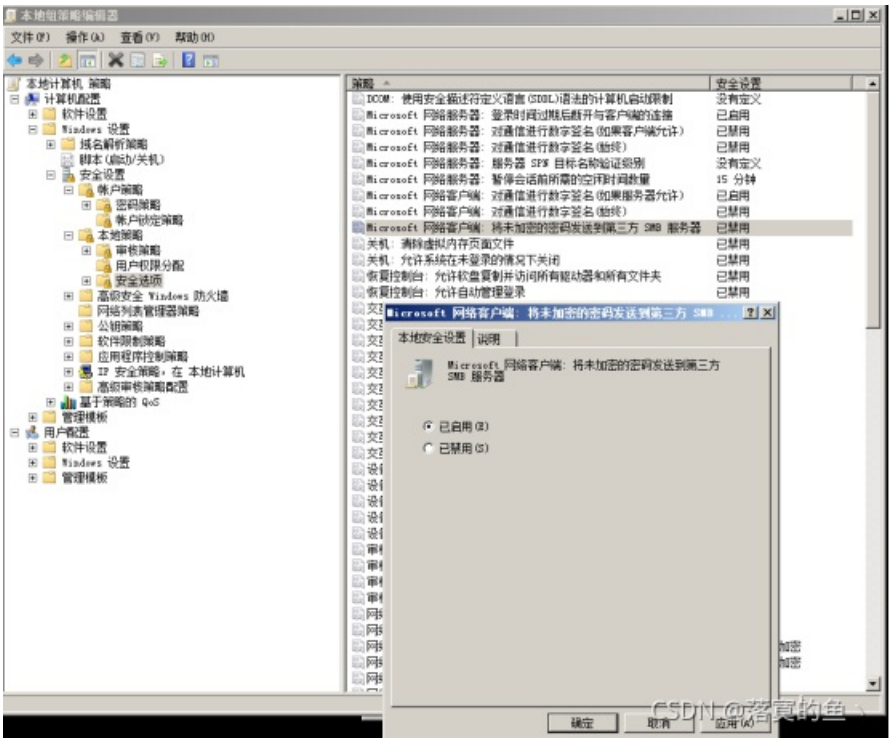
3.用户安全管理(Windows)

a.禁止从远端系统强制关机，将该权限只指派给administrators组；

Windows：管理工具-本地安全策略-本地策略-用户权限分配

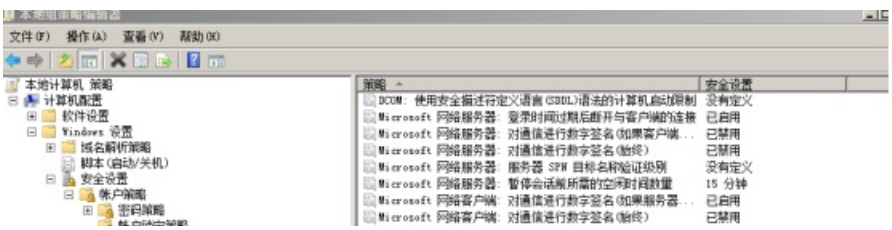


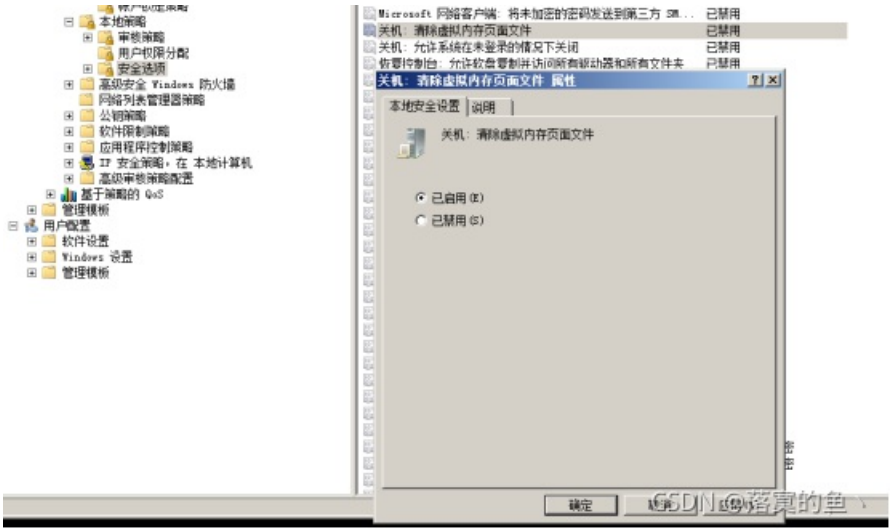
b.禁止发送未加密的密码到第三方SMB服务器。



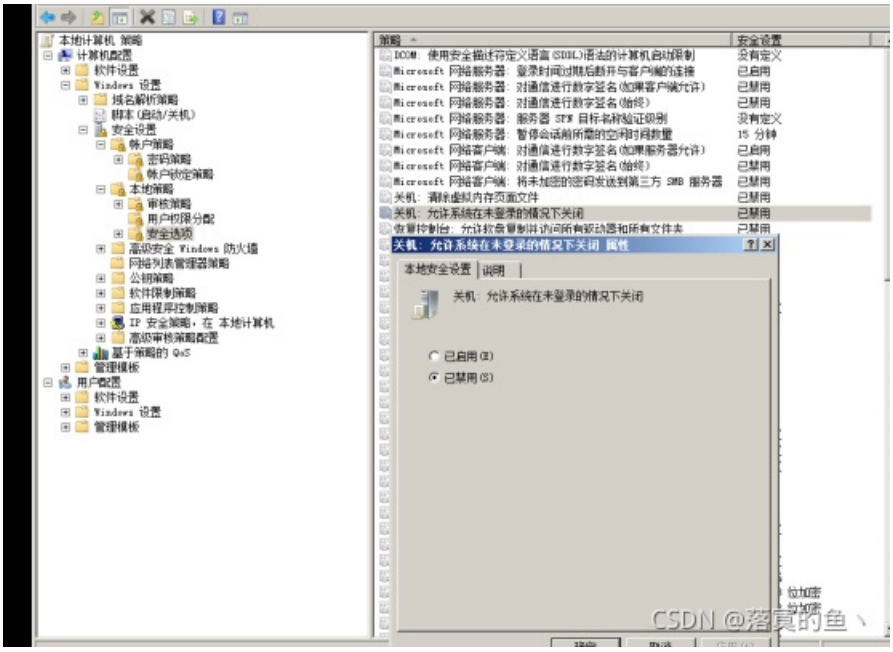
A-2任务二 本地安全策略设置（Windows）

4.关闭系统时清除虚拟内存页面文件；

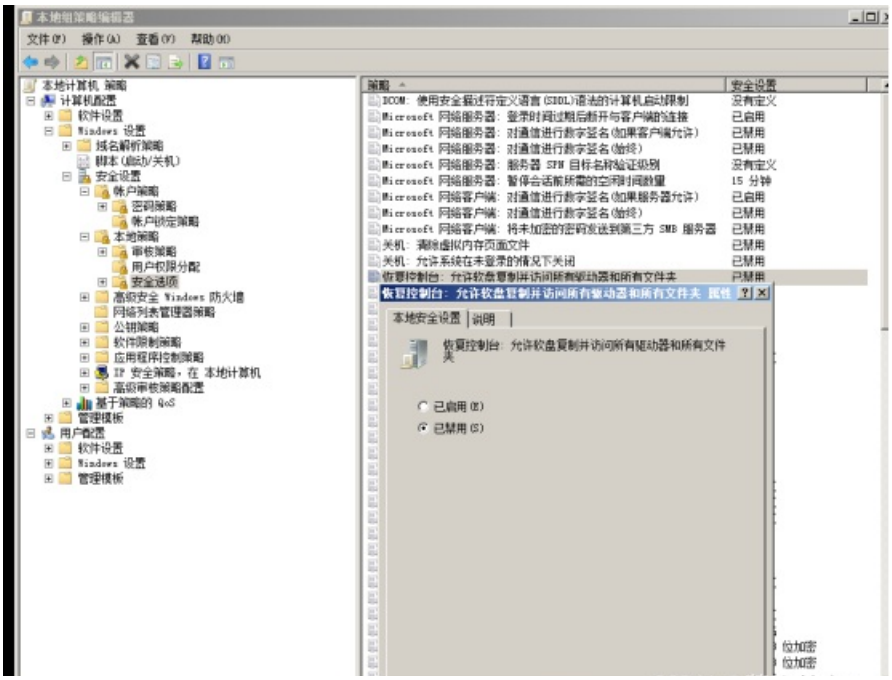




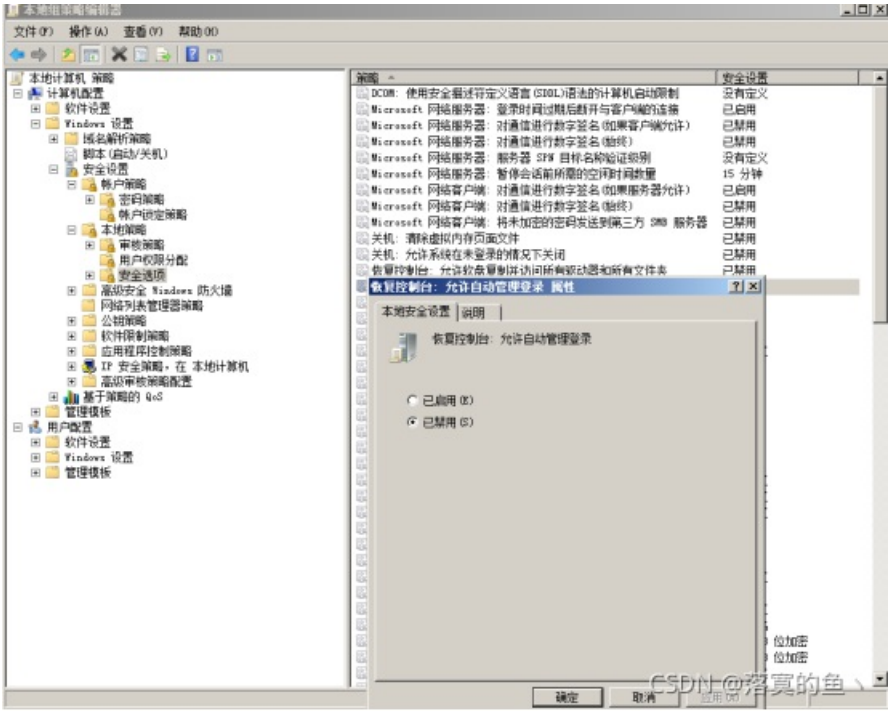
5.禁止系统在未登录的情况下关闭；



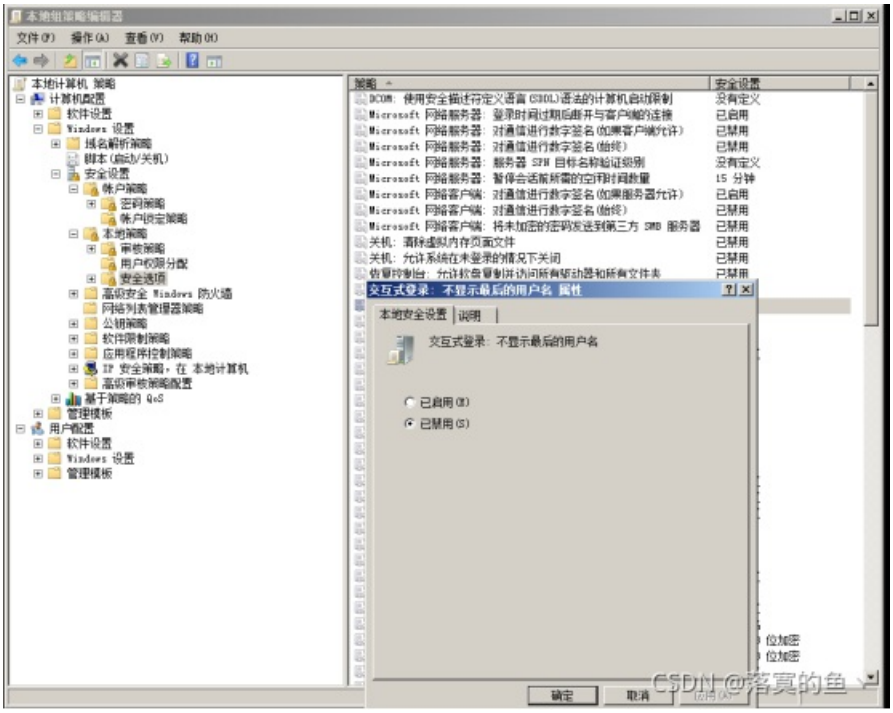
6.禁止软盘复制并访问所有驱动器和所有文件夹；



7.禁止自动管理登录；



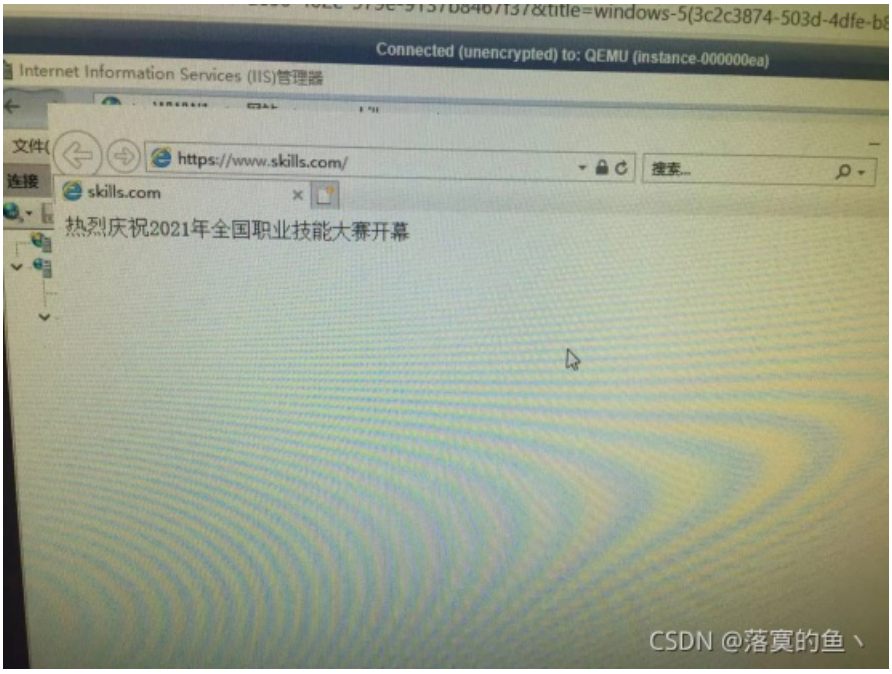
8.禁止显示上次登录的用户名。



A-3任务三 流量完整性保护（Windows）

9.创建www.chinaskills.com站点，在C:\web文件夹内中创建名称为chinaskills.html的主页，主页显示内容“热烈庆祝2021年全国职业技能大赛开幕”，同时只允许使用SSL且只能采用域名方式进行访问。

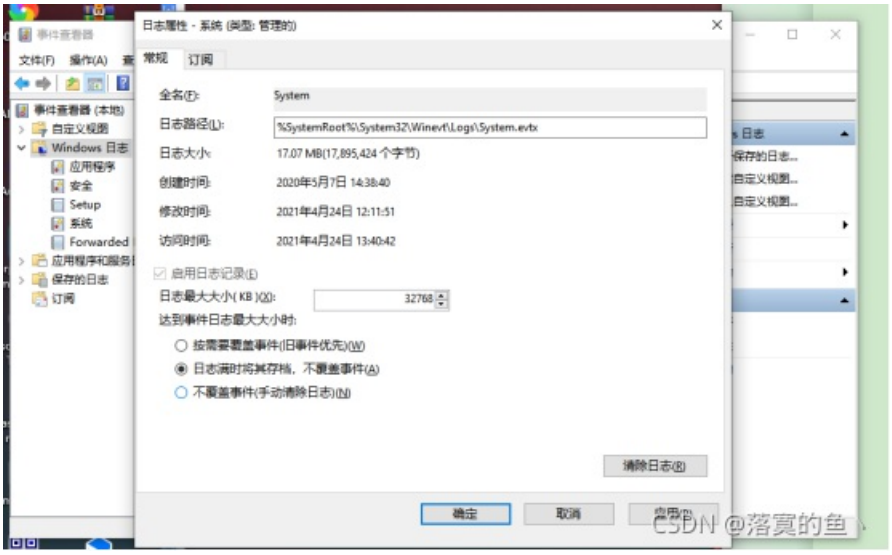
正常得web网页都是http ssl就是https 相当于加了一个证书



A-4任务四 事件监控（Windows）

10.系统日志大小至少为32MB，设置当达到最大的日志大小上限时，按需要覆盖事件。

> win+ r ： eventvwr



A-5任务五 服务加固SSH\VSFTPD\IIS（Windows, Linux）

11.SSH服务加固（Linux）

a.ssh禁止root用户远程登录；

修改配置文件 vim /etc/ssh/sshd_config

把 **PermitRootLogin yes** 改为 **PermitRootLogin no**

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
```

b.设置root用户的计划任务。每天早上7:50自动开启ssh服务，22:50关闭；每周六的7:30重新启动ssh服务。

```
crontab –e
50 7 *** /sbin/service sshd start
50 22 *** /sbin/service sshd stop
```

12.VSFTPD服务加固（Linux）；
a.设置数据连接的超时时间为2分钟；

vim /etc/vsftpd/vsftpd.conf

```
data_session_timed_out=120
```

b.站点本地用户访问的最大传输速率为1M。

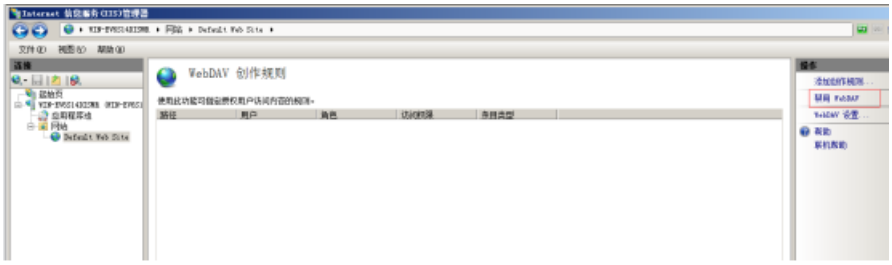
```
Local_max_rate=1M
```

13.IIS加固（Windows）；
a.防止文件枚举漏洞枚举网络服务器根目录文件，禁止IIS短文件名泄露；

```
win+ r ：regedit 打开注册表
```

HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation的值为1。直接搜索NtfsDisable8dot3NameCreation，修改其值为1。

b.关闭IIS的WebDAV功能增强网站的安全性。



A-6任务六 防火墙策略（Linux）
14.只允许转发来自172.16.0.0/24局域网段的DNS解析请求数据包；

```
iptables -A FORWARD -s 172.16.0.0/24 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -d 172.16.0.0/24 -p udp --sport 53 -j ACCEPT
```

15.禁止任何机器ping本机；

```
iptables -A INPUT -p icmp -j DROP
```

16.禁止本机ping任何机器；

```
iptables -A OUTPUT -p icmp -j DROP
```

17.拒绝 TCP 标志位全部为 1 及全部为 0 的报文访问本机；

```
iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
```

18.禁止转发来自MAC地址为29:0E:29:27:65:EF主机的数据包。

```
iptables -A INPUT -m mac --mac-source 29:0E:29:27:65:EF -j DROP
```

有问题可以私信博主哦~

最后觉得有对你有帮助话记得给个一键三连，祝大家每天开心□~