2022 年全国职业院校技能大赛（中职组）

网络安全竞赛试题

A 模块评分标准

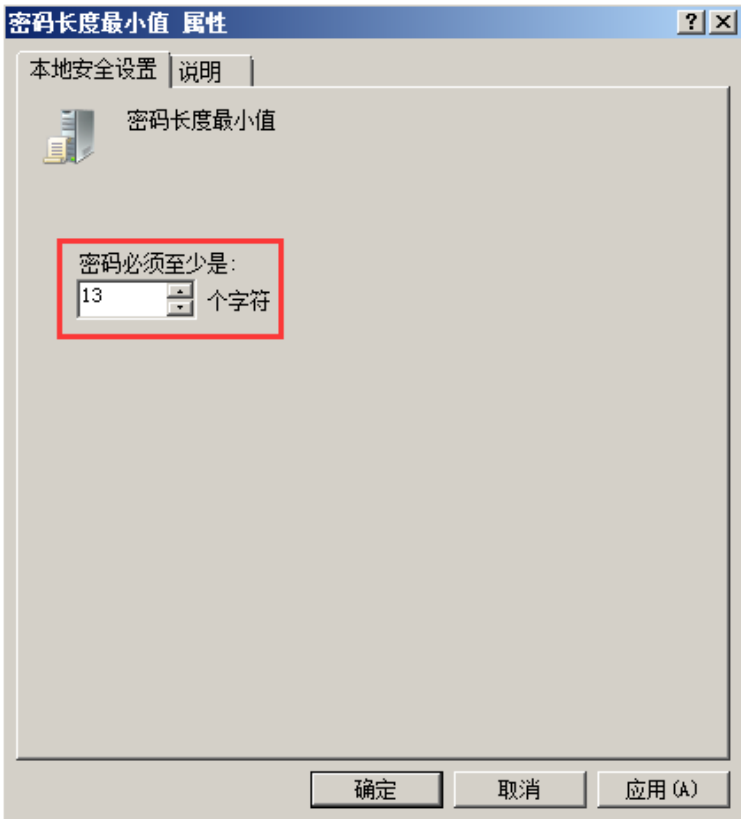
模块 A 基础设施设置与安全加固

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. 最小密码长度不少于 13 个字符（Windows），将密码长度最小值的属性配置界面截图：



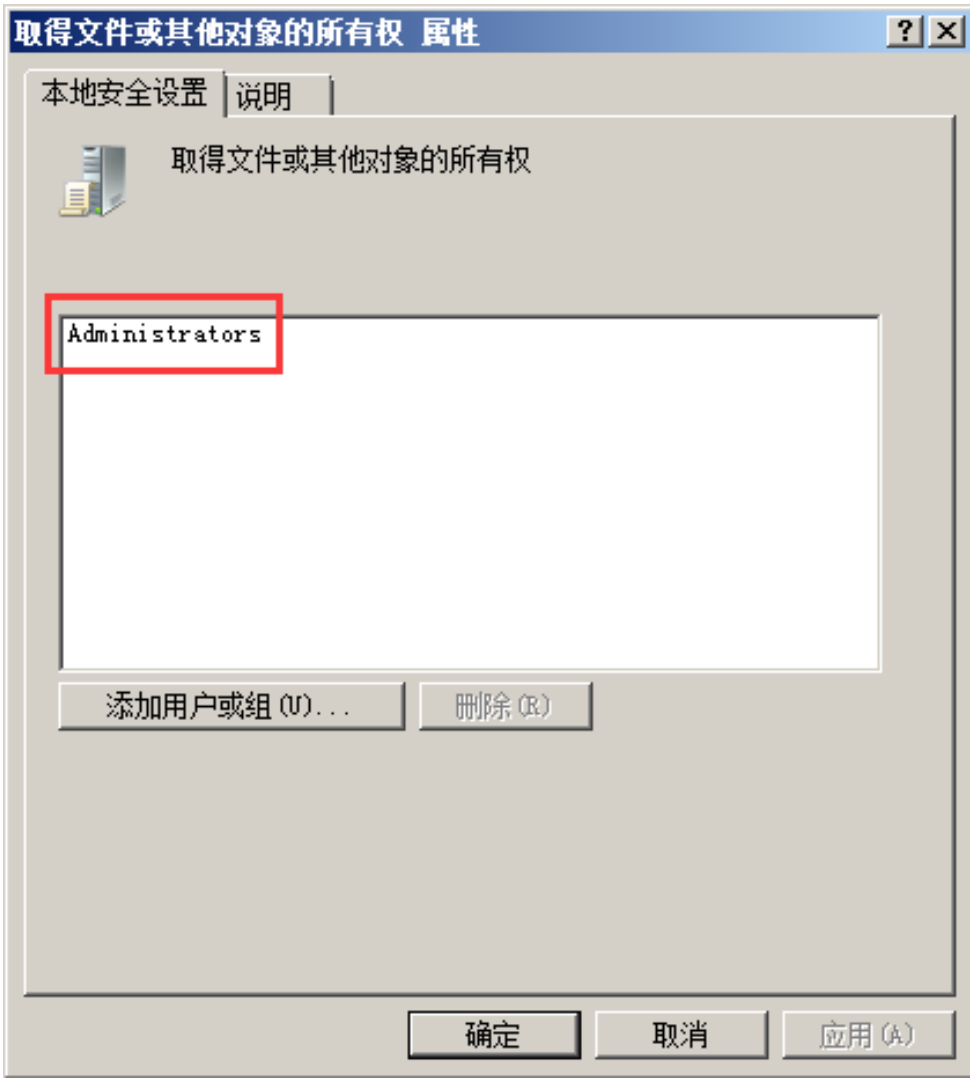
b.密码必须符合复杂性要求（Linux），将/etc/pam.d/system-auth 配置文件中对应的部分截图：

以下参数不论先后顺序，ucredit\lcredit\dcredit\ocredit

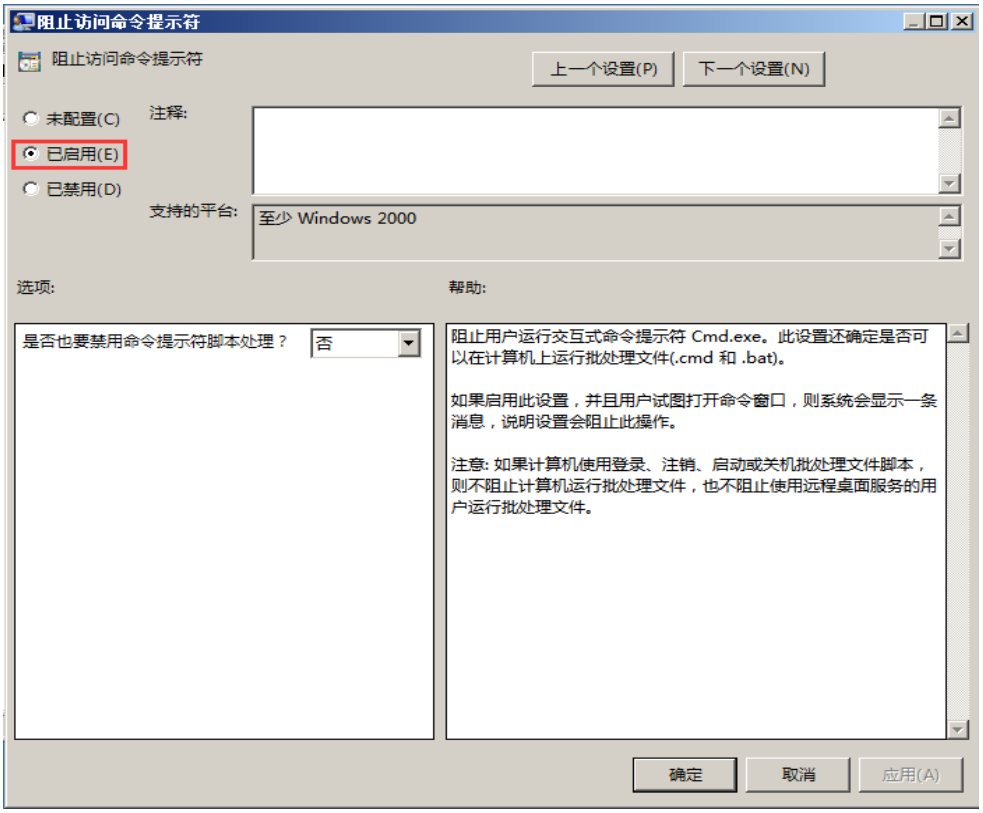
```
password    requisite     pam_cracklib.so try_first_pass retry=3 type= uc
redit=-1 lcredit=-1 dcredit=-1 ocredit=-1
```

2.用户安全管理(Windows)

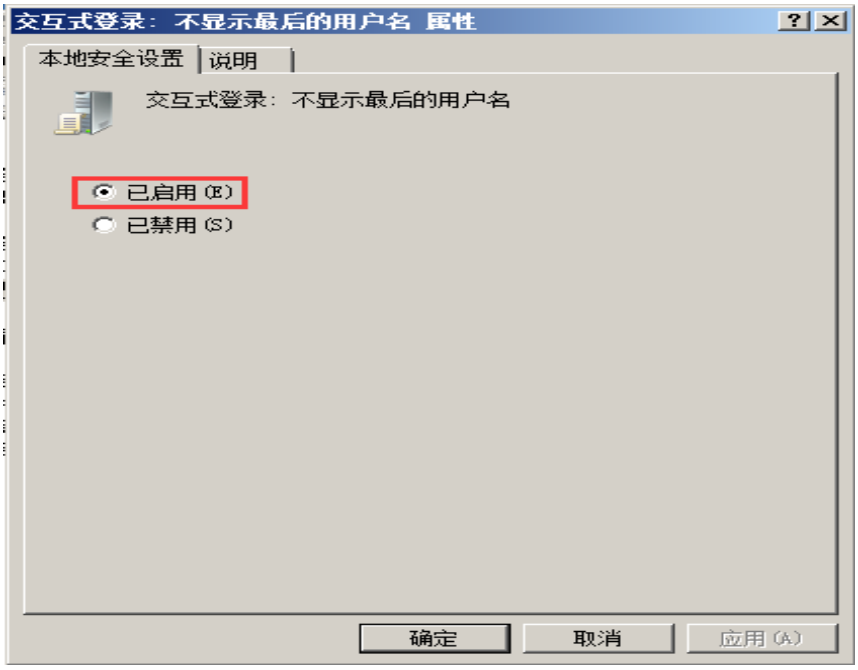
a.设置取得文件或其他对象的所有权，将该权限只指派给 administrators 组，将取得文件或其它对象的所有权属性的配置界面截图：



b. 禁止普通用户使用命令提示符，将阻止访问命令提示符配置界面截图：



c. 设置不显示上次登录的用户名，将交互式登录：不显示最后的用户名属性配置界面截图：



A-2 任务二 Nginx 安全策略（Linux）

1.禁止目录浏览和隐藏服务器版本和信息显示，将 /etc/nginx/nginx.conf 配置文件相关配置项截图：

```
server tokens  off;
```

2.限制 HTTP 请求方式，只允许 GET、HEAD、POST，将 /etc/nginx/conf.d/default.conf 配置文件相关配置项截图：

```
if ($request_method !~ ^(GET|HEAD|POST)$ ) {
    return 501;
}
```

3.设置客户端请求主体读取超时时间为 10，将 /etc/nginx/nginx.conf 配置文件相关配置项截图：

```
client_body_timeout 10;
```

4.设置客户端请求头读取超时时间为 10，将 /etc/nginx/nginx.conf 配置文件相关配置项截图：

```
client_header_timeout 10;
```

5.将 Nginx 服务降权，使用 www 用户启动服务，将 /etc/nginx/nginx.conf 配置文件相关配置项截图：

以下两张图片只要选手的截图中任意一张图与之相符即可给分

图一

```
user www www;
```

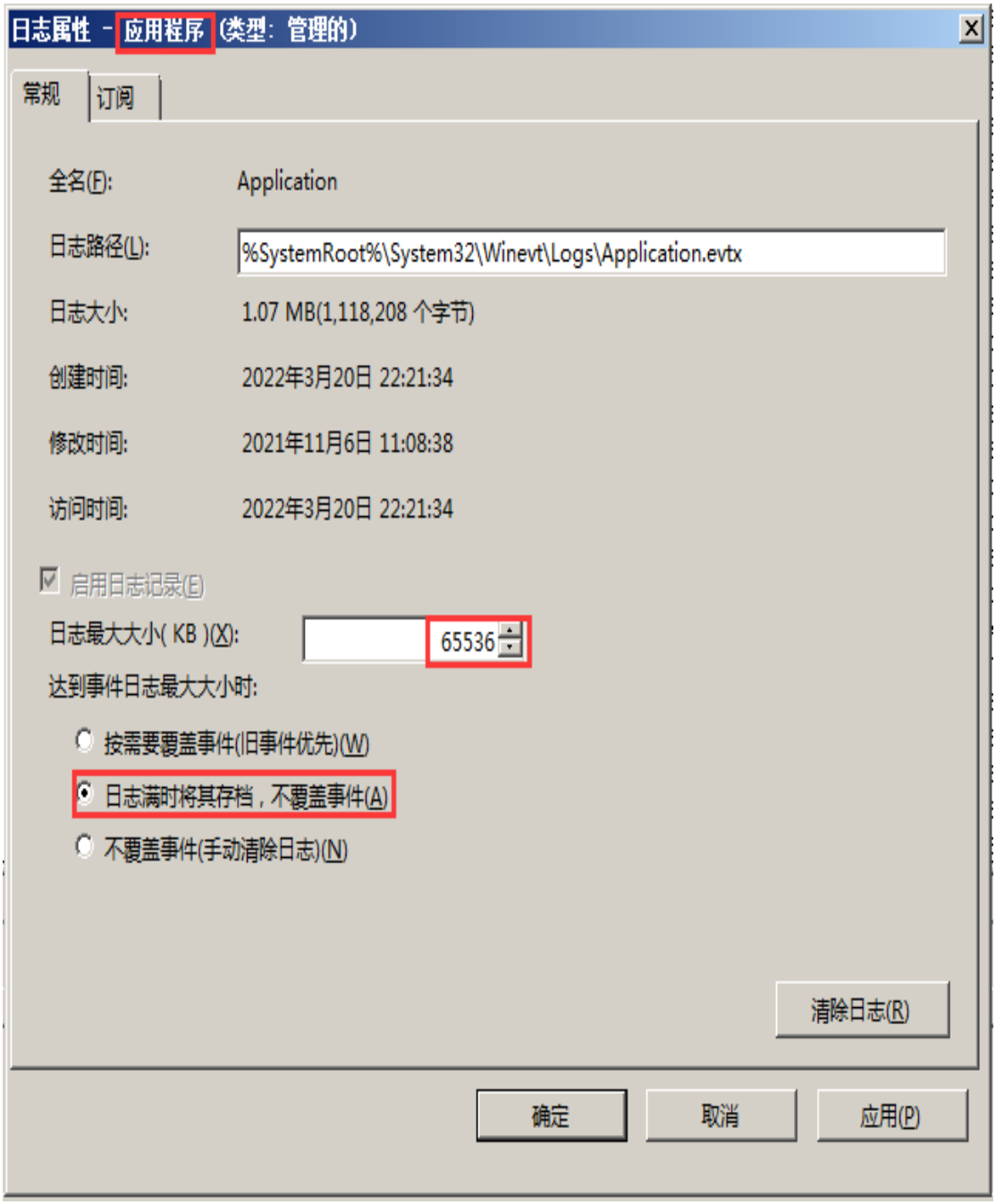
图二

```
user www;
```

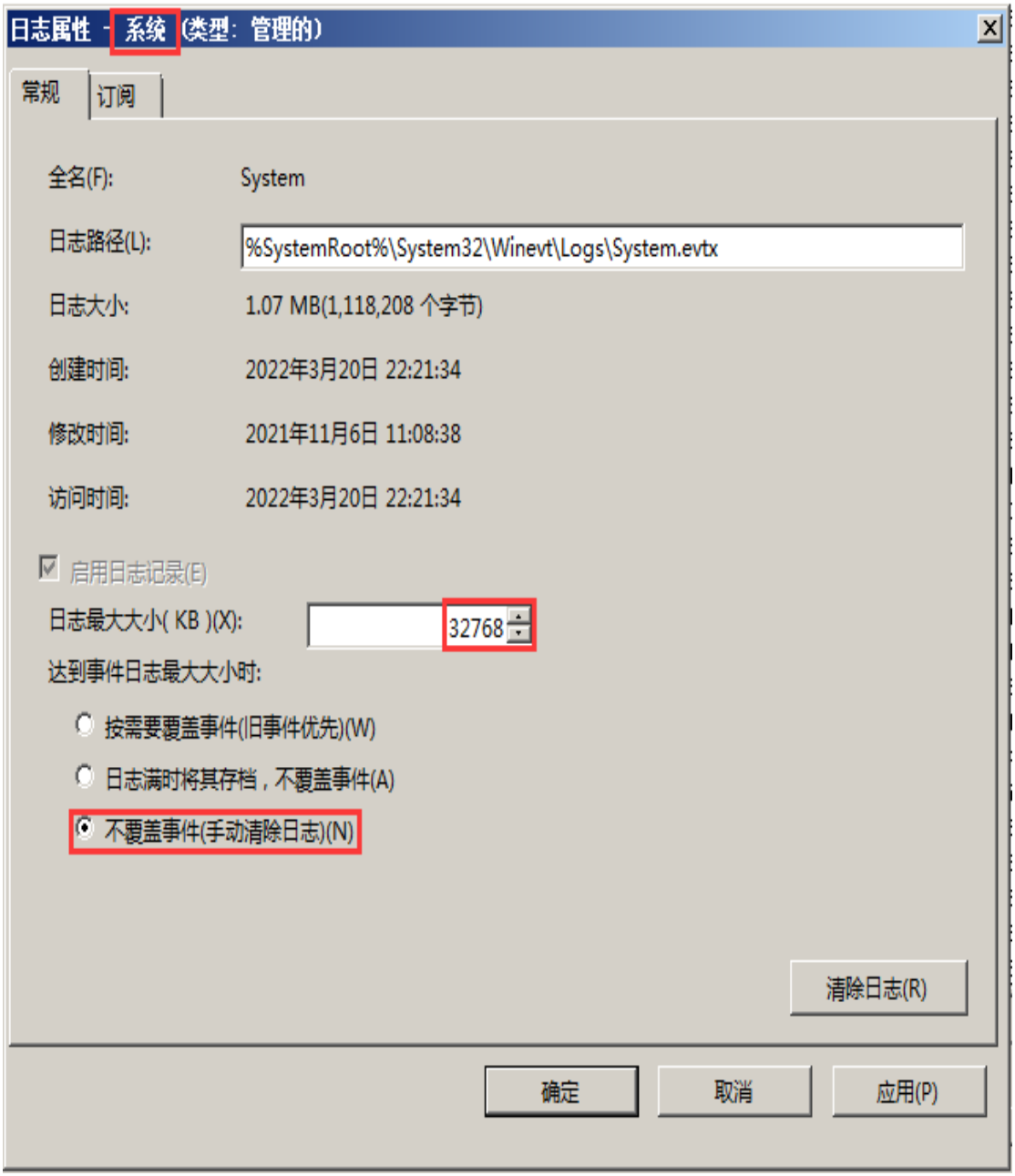
A-3 任务三 日志监控（Windows）

1.安全日志文件最大大小为 128MB，设置当达到最大的日志大小上限时，按需要覆盖事件（旧事件优先），将日志属性-安全（类型：管理的）配置界面截图：

2.应用日志文件最大大小为64MB，设置当达到最大的日志大小上限时将其存档，不覆盖事件，将日志属性-应用程序（类型：管理的）配置界面截图：



3.系统日志文件最大大小为32MB，设置当达到最大的日志大小上限时，不覆盖事件（手动清除日志），将日志属性-系统（类型：管理的）配置界面截图：



A-4 任务四 中间件服务加固 SSHD\VSFTPD\IIS（Windows，Linux）

1. SSH 服务加固（Linux）

a. 修改 ssh 服务端口为 2222，使用命令 netstat -anltp | grep sshd 查看 SSH 服务端口信息，将回显结果截图：

```
[root@localhost Desktop]# netstat -anltp | grep sshd
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN      3710/sshd
tcp        0      0 :::2222                 :::*                    LISTEN      3710/sshd
[root@localhost Desktop]#
```

b. ssh 禁止 root 用户远程登录，将/etc/ssh/sshd_config 配置文件中对应的部分截图：

```
PermitRootLogin no
```

c. 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，使用命令 crontab -l，将回显结果截图：

```
50 7 * * * /etc/init.d/sshd start
50 22 * * * /etc/init.d/sshd stop
30 7 * * 6 /etc/init.d/sshd restart
```

d. 修改 SSHD 的 PID 档案存放地，将/etc/ssh/sshd_config 配置文件中对应的部分截图：重接

```
PidFile /root/sshd.pid
```

2. VSFTPD 服务加固（Linux）

a. 设置运行 vsftpd 的非特权系统用户为 pyftp，将 /etc/vsftpd/vsftpd.conf 配置文件下的相关配置项截图：

```
nopriv_user=pyftp
```

b.限制客户端连接的端口范围在50000-60000，将/etc/vsftpd/vsftpd.conf配置文件下的相关配置项截图：

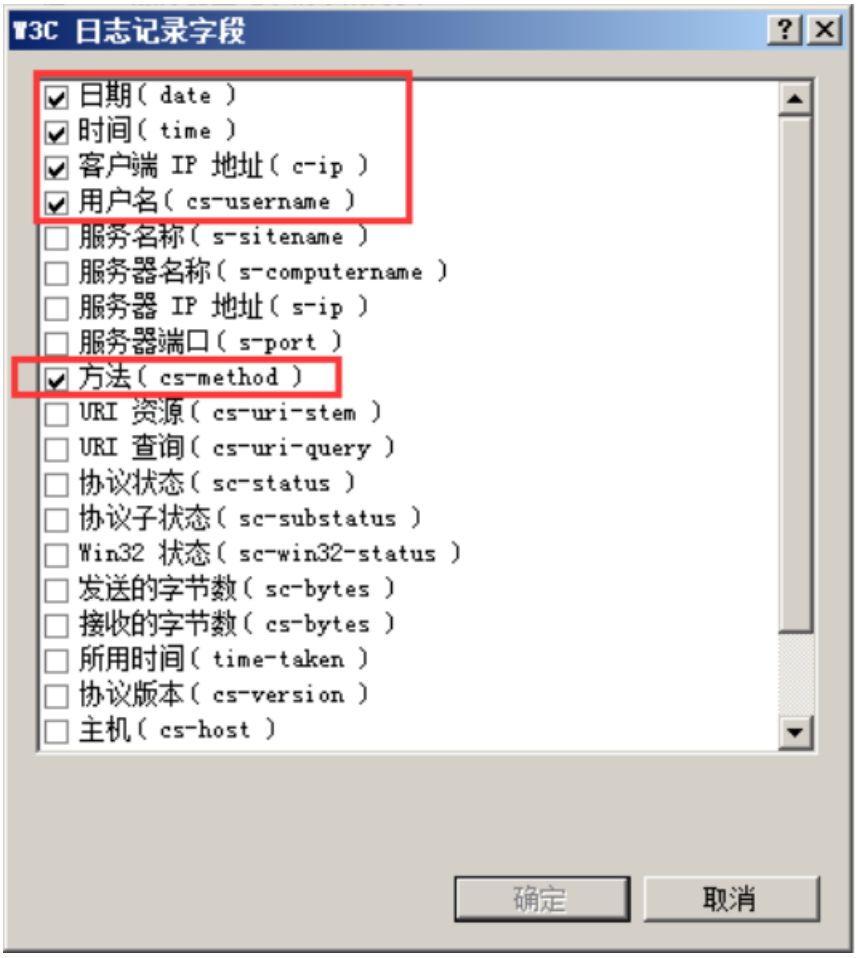
```
pasv_min_port=50000
pasv_max_port=60000
```

c.限制本地用户登录活动范围限制在home目录，将/etc/vsftpd/vsftpd.conf配置文件下的相关配置项截图：

```
chroot_local_user=YES
```

3.IIS加固（Windows）

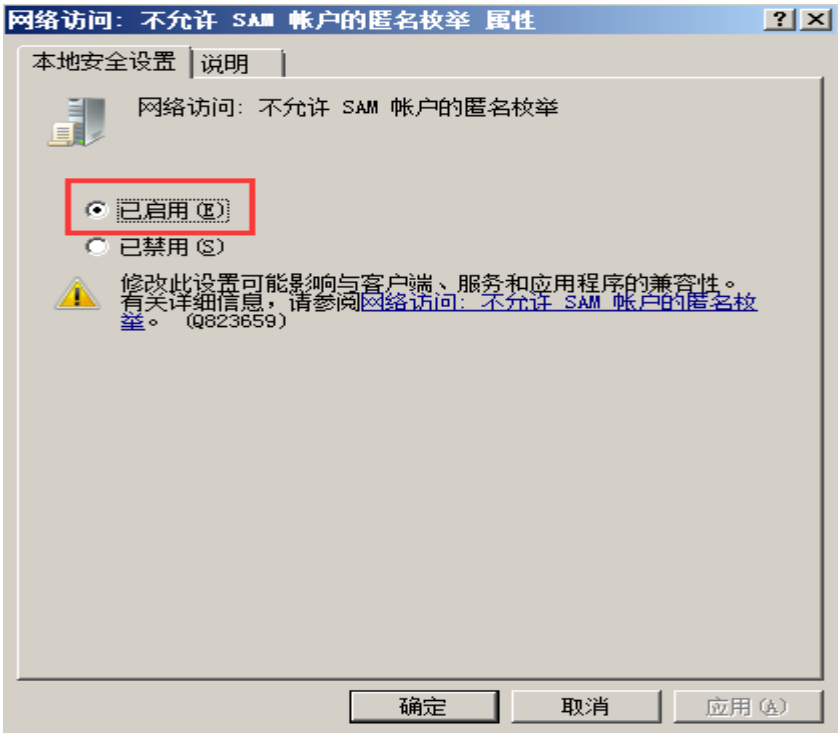
a.开启IIS的日志审计记录(日志文件保存格式为W3C,只记录日期、时间、客户端IP地址、用户名、方法),将W3C日志记录字段配置页面截图：



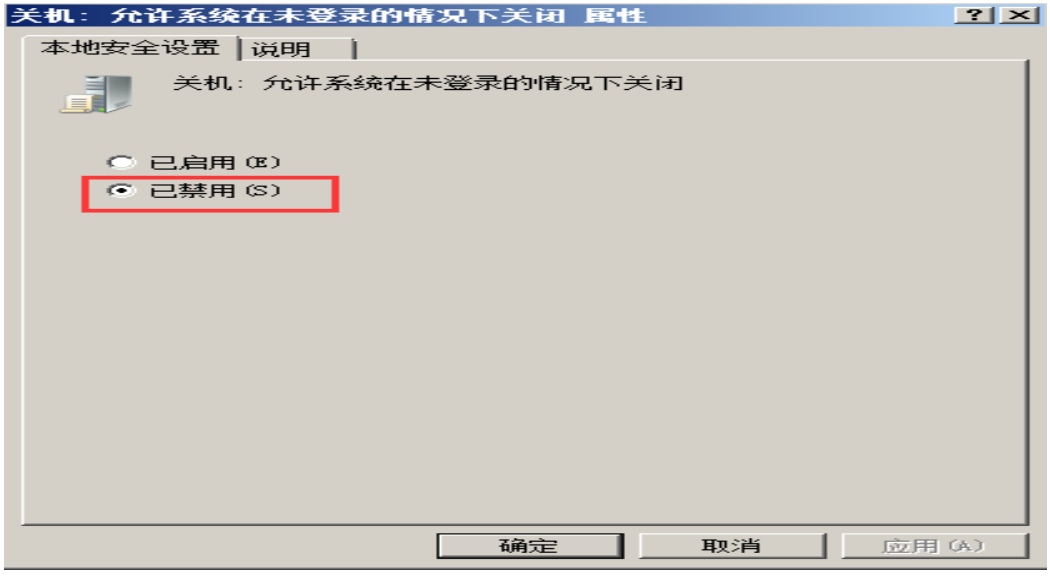
b.关闭 IIS 的 WebDAV 功能增强网站的安全性，将警报提示信息截图：

A-5 任务五 本地安全策略（Windows）

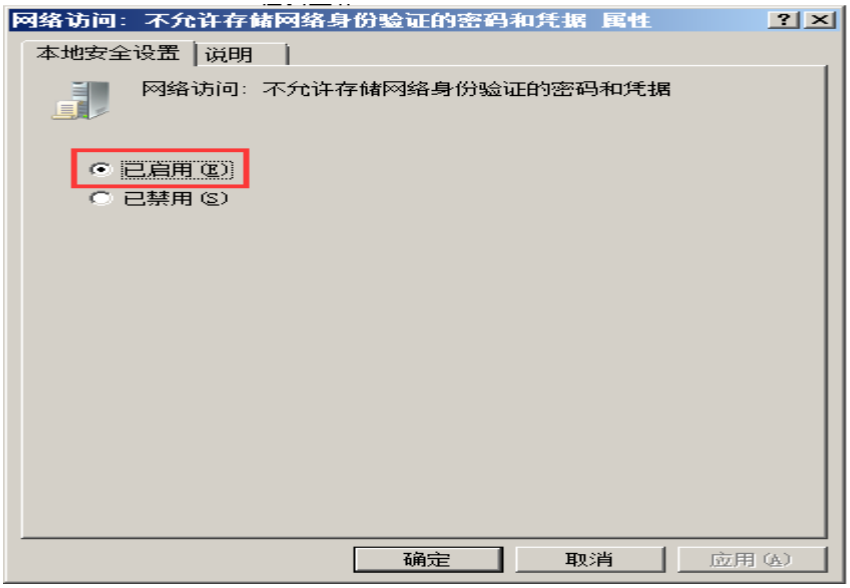
1.禁止匿名枚举 SAM 帐户，将不允许 SAM 账户的匿名枚举的属性配置界面截图：



2. 禁止系统在未登录的情况下关闭，将允许系统在未登录的情况下关闭的属性配置界面截图：

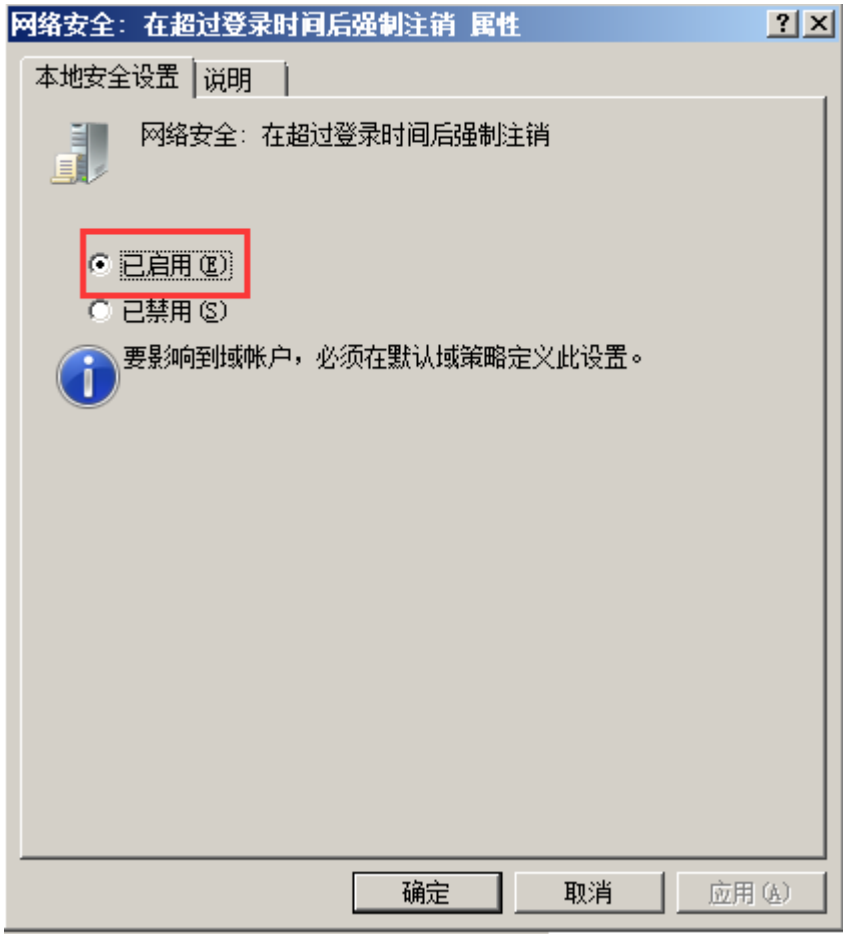


3. 禁止存储网络身份验证的密码和凭据，将不允许存储网络身份验证的密码和凭据的属性配置界面截图：



4. 禁止将 Everyone 权限应用于匿名用户，将 Everyone 权限应用于匿名用户的属性配置界面截图：

5.在超过登录时间后强制注销，将在超过登录时间后强制注销的属性配置界面截图：



A-6 任务六 防火墙策略（Linux）

1.设置防火墙允许本机转发除 ICMP 协议以外的所有数据包，将 iptables 配置命令截图：

```
iptables -A FORWARD ! -p icmp -j ACCEPT
```

2.为防止 SSH 服务被暴力枚举，设置 iptables 防火墙策略仅允许 172.16.10.0/24 网段内的主机通过 SSH 连接本机，将 iptables 配置命令截图：

```
iptables -A INPUT -p tcp --dport 22 -s 172.16.10.0/24 -j ACCEPT
```

3.为防御拒绝服务攻击，设置 iptables 防火墙策略对传入的流量进行过滤，限制每分钟允许 3 个包传入，并将瞬间流量设定为一次最多处理 6 个数据包（超过上限的网络数据包将丢弃不予处理），将 iptables 配置命令截图：

以下两张图片只要选手的截图中任意一张图与之相符即可给分

图一

```
iptables -A INPUT -m limit --limit 3/m --limit-burst 6
```

图二

```
iptables -A INPUT -m limit --limit 3/minute --limit-burst 6
```

4.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，将 iptables 配置命令截图：

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