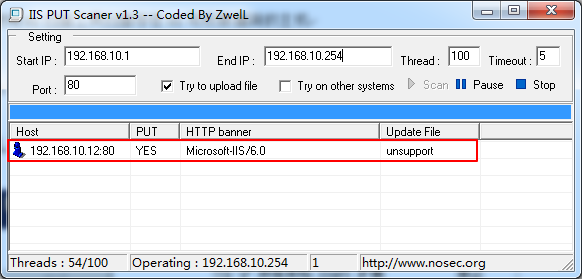
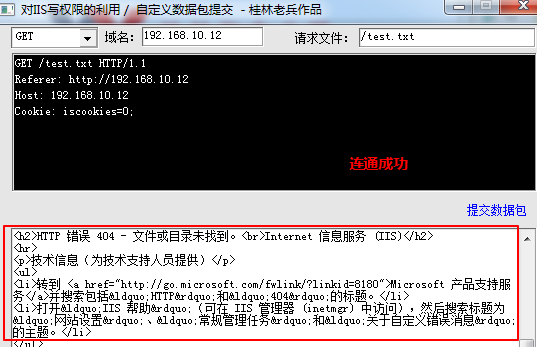
# IIS写权限拿webshell

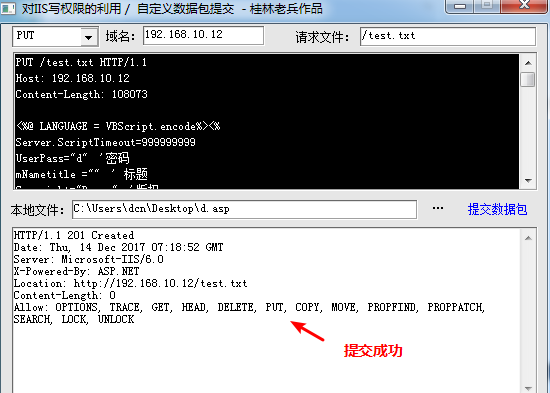
使用IIS扫描工具扫描存在IIS写权限漏洞的主机



使用桂林老兵利用工具，使用GET请求测试连通性



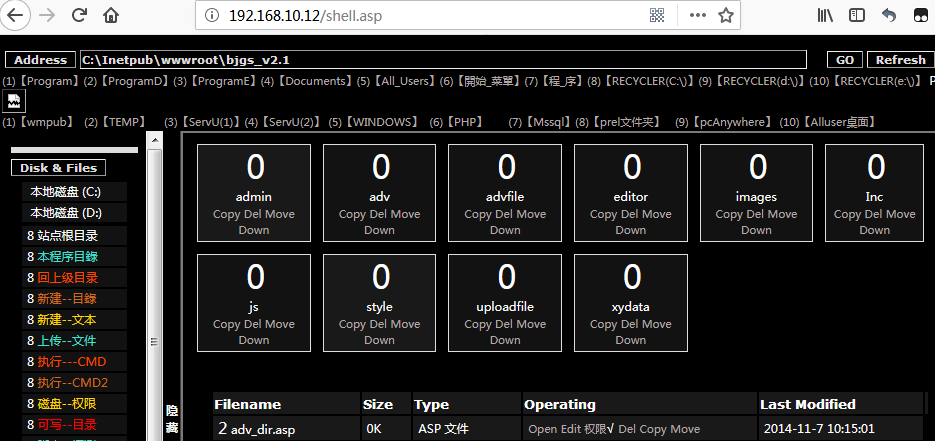
选择PUT请求，将大马上传上去



选择MOVE请求，将txt格式的文件改成asp格式的文件

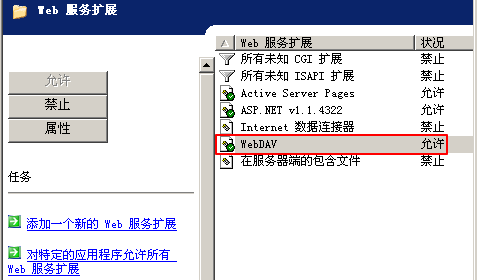


最后连接大马拿webshell

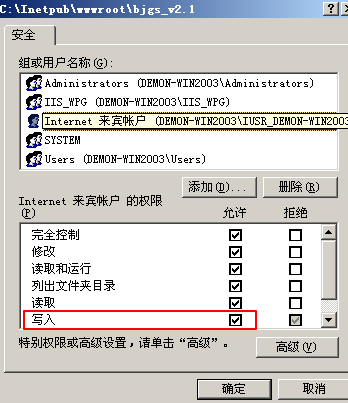


IIS写权限漏洞，主要由于管理员配置不当造成的，如下图为漏洞的形成条件：

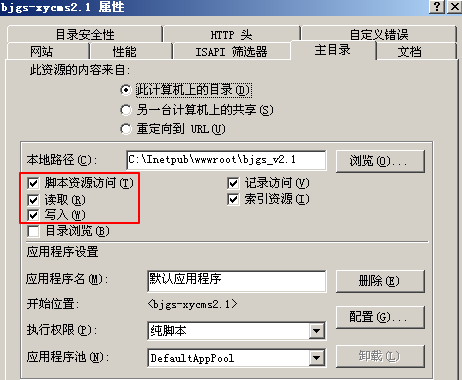
### 1.扩展模块webdav被开启啊



### 2.来宾用户有写入权限



### 3. 服务权限可以访问资源和写入



满足这三条就会产生IIS写权限漏洞，如果缺少了脚本资源访问权限，无法使用MOVE请求

另外桂林老兵PUT上去和MOVE修改后的文件是带只读隐藏属性的

