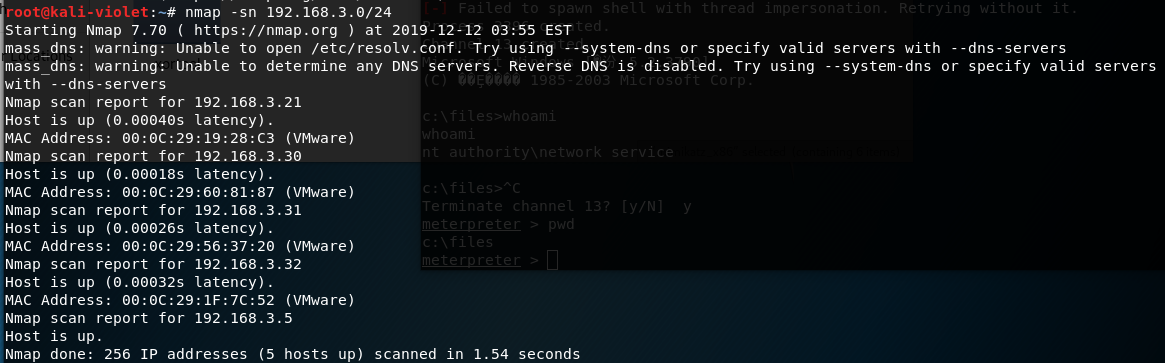
# God.org单域环境攻略(三)

## 主机探测

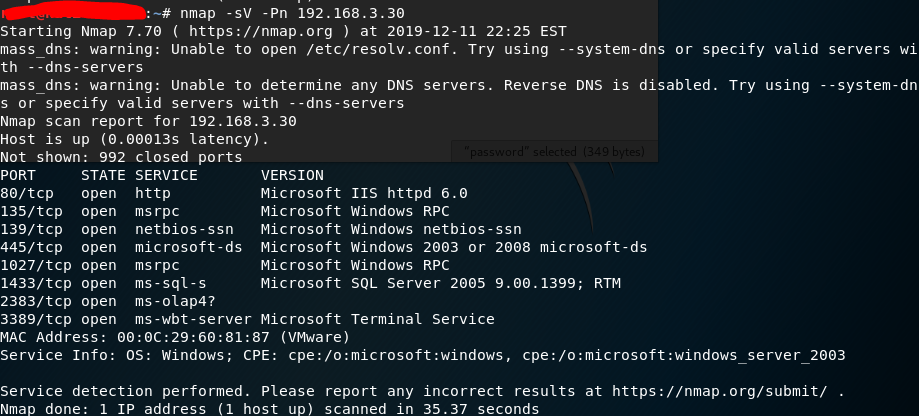
1. 探测局域网内存活的主机，发现有5台存活主机。可能有人会注意到扫描出的IP比“God.org单域环境攻略（一）”中多，那是因为不同时间段实验环境中开机的机器不同。



## 目标

**拿到192.168.3.30目标机器的SHELL。**

首先，针对192.168.3.30主机进一步探测，其他主机将在后续攻略中逐步研究。



安装了IIS 6.0服务，考虑CVE-2017-7269远程代码执行漏洞；发现主机上开启了445端口，考虑探测是否存在永恒之蓝漏洞；安装了mssql漏洞，考虑弱口令；3389端口打开，考虑cve-2019-0708远程桌面代码执行漏洞；主机是windows 2003,考虑是否存在ms08-067漏洞。

## 本地服务攻击

以下所有操作都假设首次尝试突破目标机器192.168.3.30，非首次攻破可收集主机信息，然后做出下一步操作，后续文章再介绍。

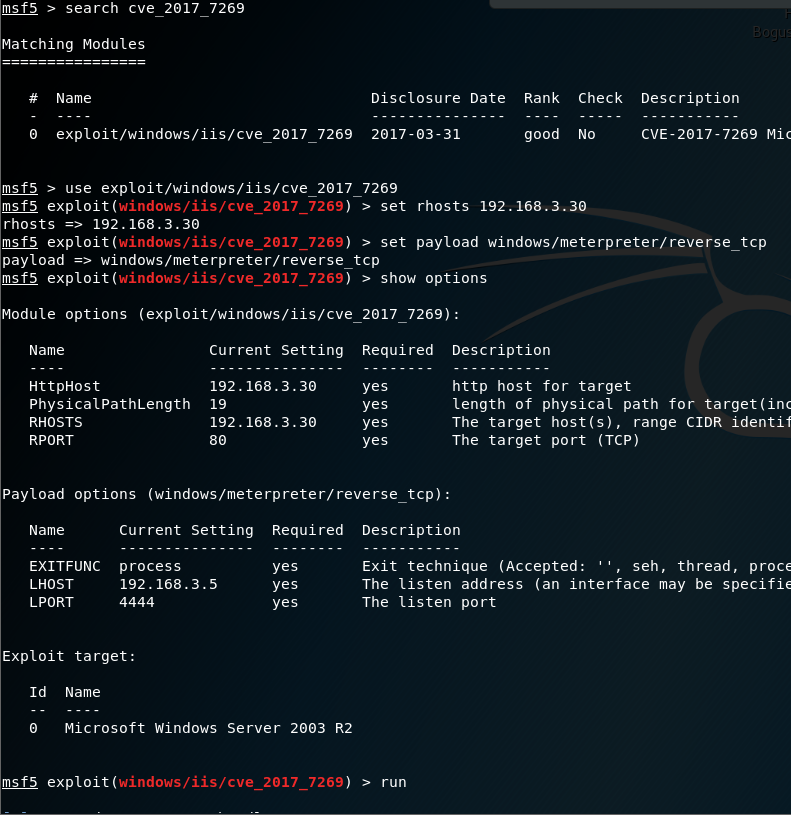
### CVE-2017-7269漏洞

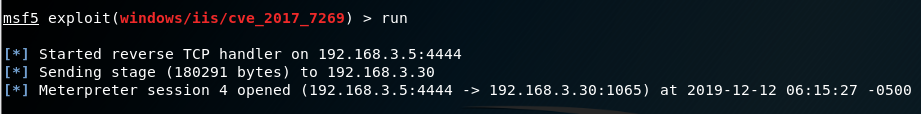
我们的目标机器是安装了iis 6.0的windows 2003主机，因此着重关注iis 6.0爆出的远程代码执行漏洞。CVE-2017-7269是IIS 6.0上存在的缓存区溢出漏洞，可以在windows 2003上远程代码执行，尝试用该漏洞的exp打目标主机。

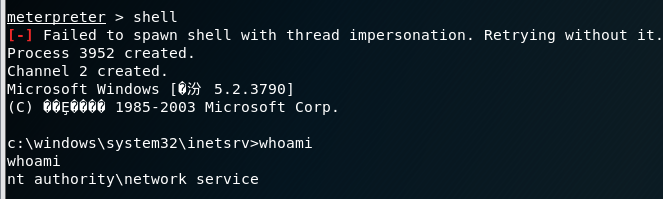
Kali的msf框架中没有集成该漏洞的利用脚本，从网上下载 [<https://github.com/zcgonvh/cve-2017-7269>，然后将[cve-2017-7269.rb](https://github.com/zcgonvh/cve-2017-7269/blob/master/cve-2017-7269.rb)拷贝到kali](https://github.com/edwardz246003/IIS_exploit，然后将exploit.py拷贝到kali)的/usr/share/metasploit-framework/modules/exploits/windows/iis目录下，记得修改文件的权限（同其他rb文件权限一致即可），此时还是无法搜索到该利用模块，需要在msf中reload所有模块。

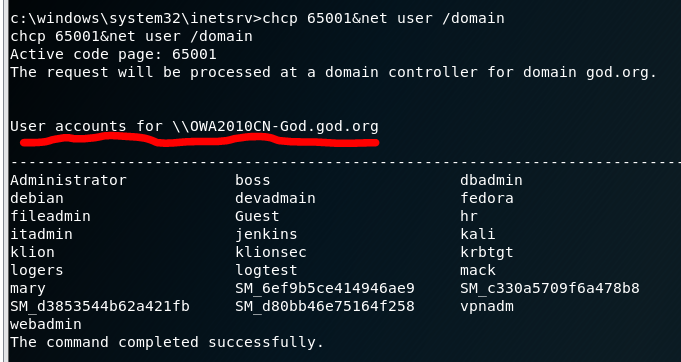


然后利用该模块进行攻击。





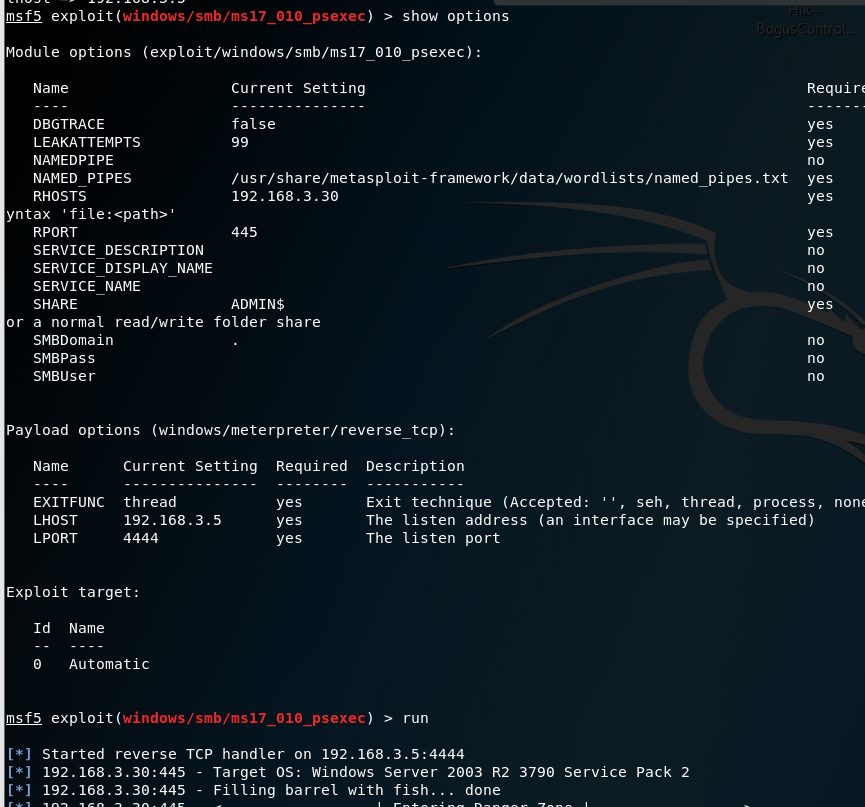


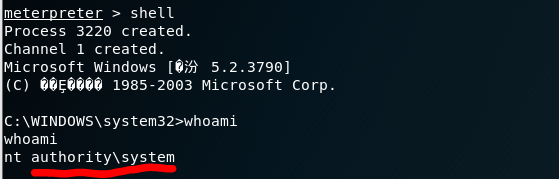


Getshell后，用命令whoami查看当前用户，发现获得一个低权限的shell,然而，是一个域内用户，太棒了！！！后面得好好利用。

### 永恒之蓝漏洞

目标主机上开启了445端口，利用kali集成的msf中自带的ms17\_010利用模块尝试利用。过程同“God.org单域环境攻略(二)”，此处不再赘述。值得注意的是，继续使用windows/smb/ms17\_010\_eternalblue利用模块，发现无法成功，这时换一个payload即可（例如：windows/smb/ms17\_010\_psexec），获得的shell权限是system权限，相较于利用IIS漏洞getshell，拿到的权限更大。





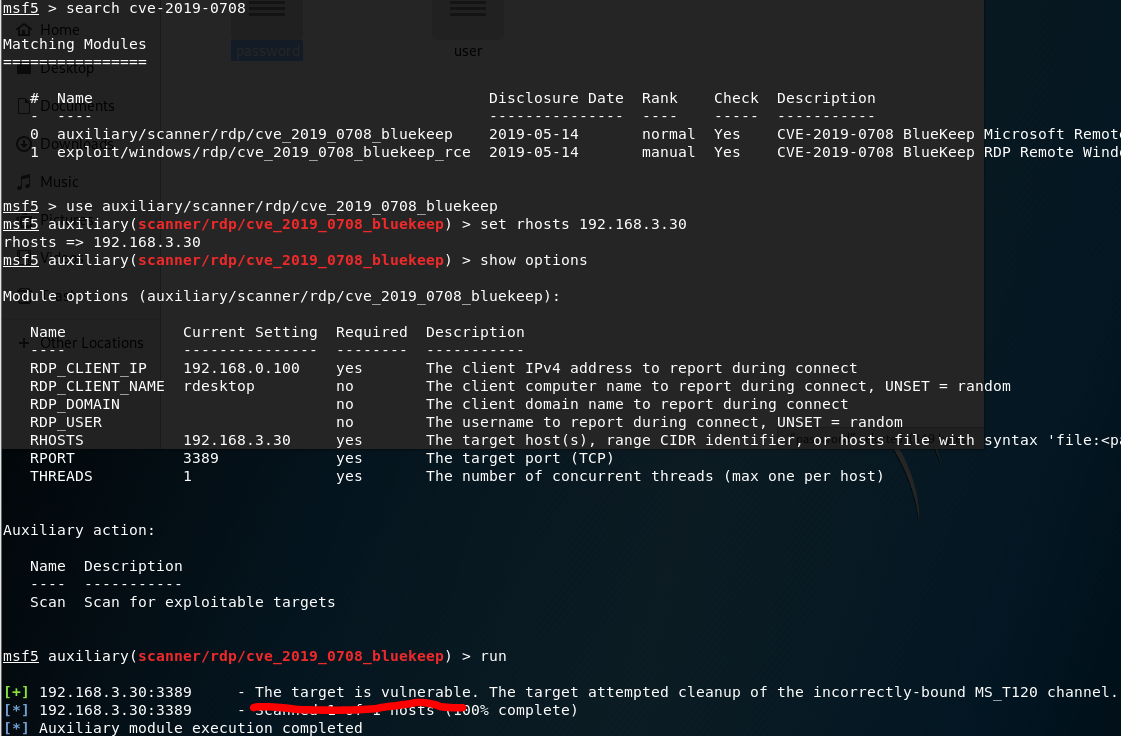
### mssql弱口令

经过测试发现目标系统mssql服务为弱口令“sa\admin”,也可以进行远程代码执行，同“God.org单域环境攻略(二)”，获得的shell亦是system权限。

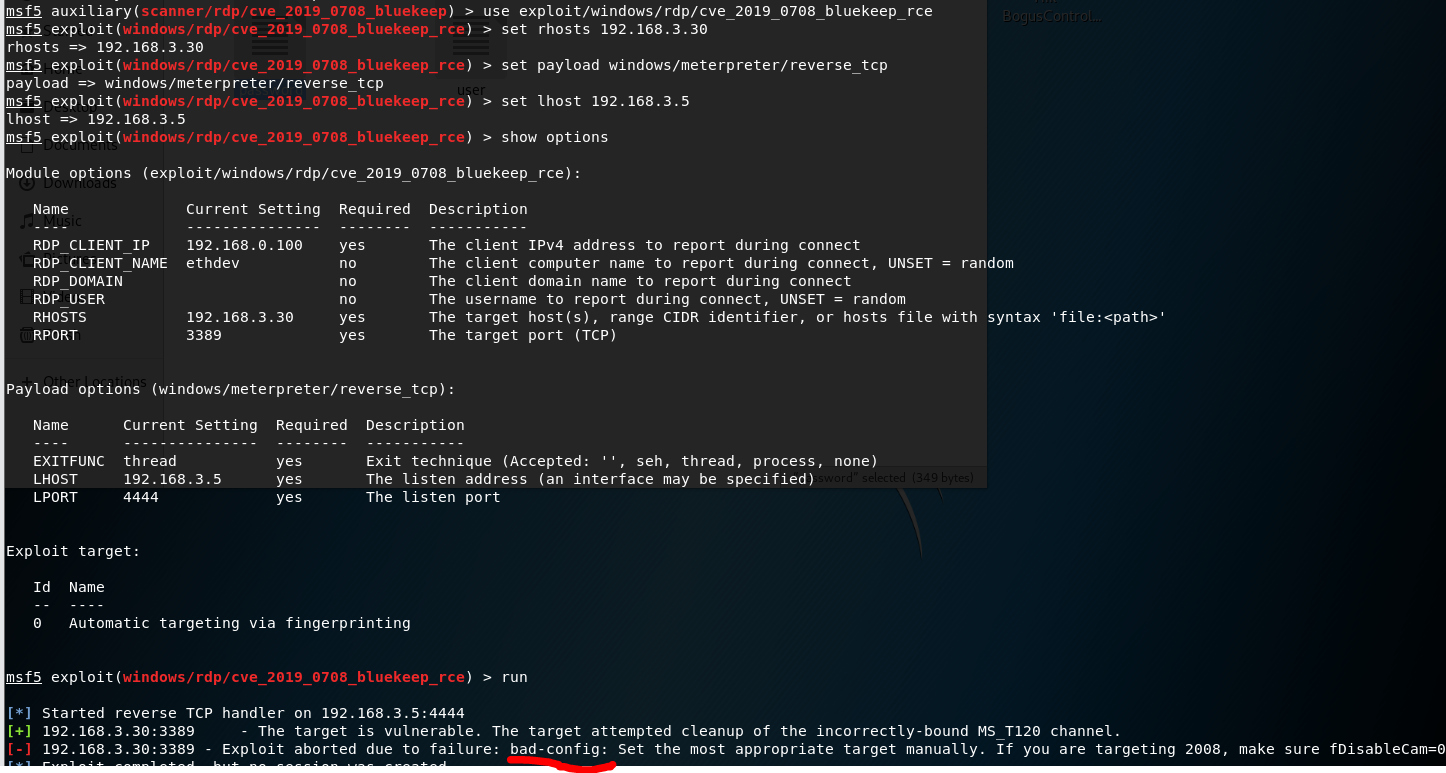
### CVE-2019-0708

目标主机打开了3389端口，且该漏洞影响win 7、win Server 2008 R2、win Server 2008、win Server 2003、win XP。用kali自带的msf框架尝试利用该漏洞攻击目标主机。

首先使用auxiliary/scanner/rdp/cve\_2019\_0708\_bluekeep模块探测目标主机是否存在该漏洞，结论是存在。



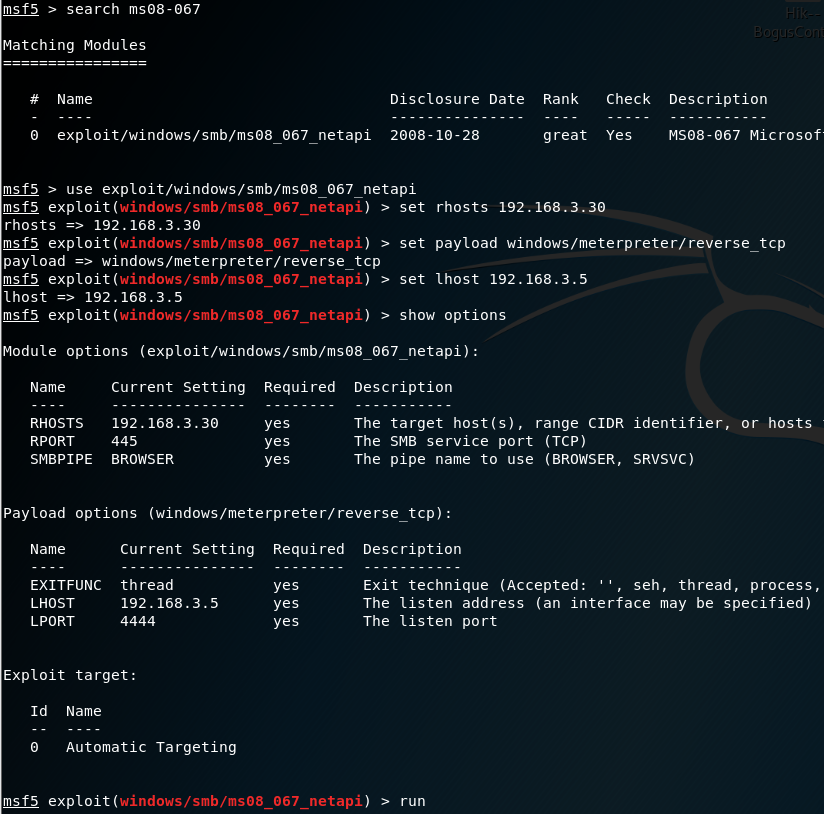
进一步使用windows/rdp/cve\_2019\_0708\_bluekeep\_rce模块利用该漏洞，失败。



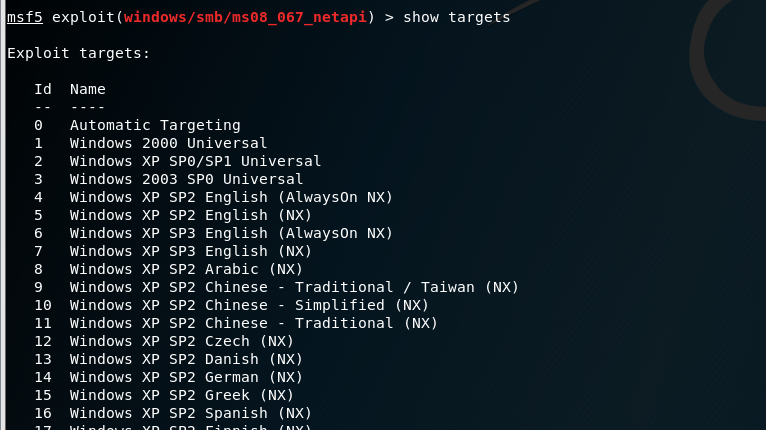
进一步分析失败的原因，该利用模块仅支持win7 sp1和win 2008 r2。这时可以在网上搜一个msf的exp再次尝试攻击。

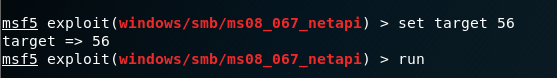
### ms08-067

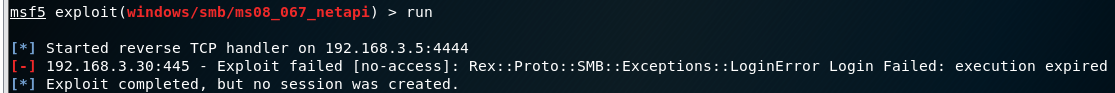
ms08-067是利用smb协议（445端口）的缓冲区溢出漏洞，它影响Windows 2000/XP/Server 2003/Vista/Server 2008的各个版本，除了Windows Server 2008 Core系统。因此考虑目标机器是否存在该漏洞。



此处target使用的是自动，我们亦可自行设置







经过测试，无论选择何种target,都没有利用成功。

## 总结

拿到目标机器的shell并不表示攻击结束，横向渗透是后续工作的重点关注对象，在以后的文章中会详细介绍。