

Author: bugcx or Anonymous

Url:



作者: Hilven

目录

本次目标的环境.

- 1.1 内网网络拓图以及平台介绍.
- 1.2 渗透测试的目的.
- 1.3 此次渗透目标内容和范围.
- 1.4 规避的风险.

二、此次内网渗透过程

- 2.1 内网突破 (Socket 端口转发以及终端连接) .
- 2.2 系统口令获取, Hash 破解, 管理软件密码破解.
- 2.3 社会工程学以及密码习惯组合字典扫描收集管理信息.
- 2.4 内网常用的 IPC\$ 共享入侵.
- 2.5 ARP 探测以及 ARP 挂马突破员工 PC.
- 2.6 ERP 内部员工办公系统挂马 (Internet Explorer Aurora Exploit 2010-01-17) 利用.
- 2.7 利用同步数据软件进行渗透 .
- 2.8 利用 IIS 可写权限配合 IIS6.0 文件后缀名解析漏洞进行突破.
- 2.9 利用 Windows XP 2K 远程, local Exploits, 溢出进行权限获取和提升.
- 3.0 以上方法配合反弹远程控制木马配合.
- 3.0.1 域内的 HASH 注入攻击突破 (未实现成功)

三、目标系统安全加固解决办法总结

- 3.1 访问控制.
- 3.2 电信和网络安全.
- 3.3 安全管理与实践.
- 3.4 应用和系统开发安全.

1.1

内网网络拓图以及平台介绍

目标网络规模为一个三层交换环境

IP地址分布以及业务分类

192.168.100.X-192.168.103.X 数据内部员工办公网路

176.12.1.X-176.12.15.X 为Web于数据库支持网路

192.168.11.X-192.168.11.255 为空闲网络区域

总共分为三个域 shif cyts ccit 共467台计算机。

以上信息是在渗透过程中得到的

为了方便我改写了一个批处理

代码为

```
=====domain.bat=====
```

```
@echo off
```

```
setlocal ENABLEDELAYEDEXPANSION
```

```
@FOR /F "usebackq delims=, " %%J IN (`net view /domain ^|find "命令執行成
```

功" /v ^|find "The command completed successfully." /v ^|find "命令成功完成" /v ^|find "--

```
" /v ^|find "Domain" /v ^|find "" /v ^|find "コマンドは正常に終了しました" /v /i ) do (
```

```
@echo =====domain:%%J=====
```

```
@FOR /F "usebackq eol=; delims=, " %%i in (`net view /domain:%%J ^|findstr "\\"`) DO (
```

```
@FOR /F "usebackq eol=; tokens=1,2,3* delims=\\\" %%a in (`echo %%i`) do (
```

```
@FOR /F "tokens=1,2,3,4* usebackq delims=: " %%K IN (`@ping -a -n 1 -w 100 %%a ^|findstr "Pinging"`) do (
```

```
@echo \\%%L    %%M
```

)

)

)

)

```
echo %0
```

```
=====end=====
```

```
127.0.0.1:88 自动查询各个域下计算机名字以及IP地址
C:\WINDOWS\system32\cmd.exe
\\WANGTING [172.16.9.154]
\\WANGWEI-AWARD [172.16.6.165]
\\WANGWR [172.16.7.104]
\\WANGXIN [172.16.8.178]
\\WANGYJ [172.16.9.220]
\\WANGZHENG [172.16.7.35]
\\MEIWEI [192.168.105.102]
\\WEIXIN [172.16.7.84]
\\WENJING [172.16.6.80]
\\WENSS [192.168.103.49]
\\WF [172.16.7.103]
\\MUGN [172.16.7.178]
\\MUXIAO [172.16.8.125]
\\MUXIAOQIAN [172.16.6.55]
\\MUZB-LENOVO [192.168.101.132]
\\XIANGTY [172.16.5.215]
\\XIEYUFEI [172.16.7.30]
\\XIONGXIN [172.16.5.162]
\\XIQI [172.16.9.88]
\\XUEJ [172.16.7.217]
\\XUWMEIW [192.168.102.36]
\\XUXIAOJIE [172.16.5.206]
\\XWWANG [172.17.22.43]
\\YANG-CYTS [172.16.6.152]
\\YANGCHENG [192.168.105.57]
\\YANGDONG [172.16.6.155]
\\YANGJIN [172.16.8.95]
\\YANGP-16 [172.16.8.96]
\\YANGXUAN [172.16.8.90]
\\YANL [192.168.105.50]
\\YANWEN [172.16.6.93]
\\YANYAFEI [172.16.6.86]
\\YANZH [172.16.5.200]
\\YAOSJ [172.16.7.100]
\\YAOZH [172.16.8.140]
\\YUANJING1 [172.16.6.98]
\\YUENING [192.168.101.104]
\\YUH [172.16.7.164]
\\YUJJ [192.168.105.59]
\\YULB-LENOVO [172.16.31.16]
\\YULI [172.16.9.54]
```

blog.bug.cx

系统类型,安装软件版本以及类别
Windows xp 2K以及Linux
Mssql2000 2005 Sybase IIS5.0 6.0 内网系统全部采用麦咖啡企业级个别伺服器安装了数据同步软件

1.2
渗透测试的目的
渗透测试一方面可以从攻击者的角度,检验业务系统的安全防护措施是否有效,各项安全策略是否得到贯彻落实;另一方面可以讲潜在的安全风险以真实事件的方式凸现出来,从而有助于提高相关人员对安全问题的认识水平。渗透测试结束后,立即进行安全加固,解决测试发现的安全问题,从而有效地防止真实安全事件的发生

1.3
此次渗透目标内容和范围.
此次渗透的为内容为目标数据库服务器以及员工办公PC..

1.4
规避的风险
此次渗透是在不影响目标业务工作的前提下进行测试,个别渗透测试手法已在本地搭建测试完成之后再应用到目标,以保证目标业务正常,(如ARP探嗅 ARP ERP办公系统挂马突破,其中IEOday利用测试已本地通过不会造成目标员工办公PC崩溃或者出现异常)。
此次内网渗透过程

2.1
内网突破 (Socket端口转发以及终端连接)
通过外网web服务器222.11.22.11(192.168.22.34)(假设IP)上的Web Shell,连接内网ip为192.168.22.35的Mssql2005服务器,当前账户权限为Sa。(账户密码通过查看Web.config得到) Sa账户是Mssql的默认的最高权限账户由于MSSQL服务是以SYSTEM权限运行的,而MSSQL恰巧提供了一些能够执行命令的函数加入能成功利用,会得到一个SYSTEM权限,所以我认为这会有很大机会让我利用成功

(如 xp_cmdshell xp_dirtree xp_fileexistxp_terminate_process sp_oamethod sp_oacreate xp_regaddmultistring xp_regdelete) 由于SQL 服务器处于硬防之下,一般在防火墙做的限制都是禁止外部连接内网,没有限制由内置外的连接.我们通够Socket端口转发来进行突破.本地监听如图



本地Mstsc.exe host 127.0.0.1:88

2.2系统口令获取,Hash破解,管理软件密码破解

这之前替换sethc.exe为cmd.exe程序-系统做放大镜后门得到一个CMD Shell为渗透提供方便 (在渗透完成之后所有的目标文件都已经恢复) 通过Cmd Shell连接本地Ftp Server Get Hash.exe(系统口令哈希值获取工具) VNC4密码获取工具GUI版到当前主机, 【VNC4的密码是保存在注册表中的地址 为: HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4\password】 抓取密码之后通过FTP PUT返回本机.抓取没有出现提示14位以上,直接通过在线的LM密码查询网站进行查询如:

两个常用的Hash在线破解网站

<http://cracker.offensive-security.com/index.php>

<http://www.objectif-securite.ch/en/products.php>

得到系统当前主机管理员密码为ccit2006 VNC4密码为如下图



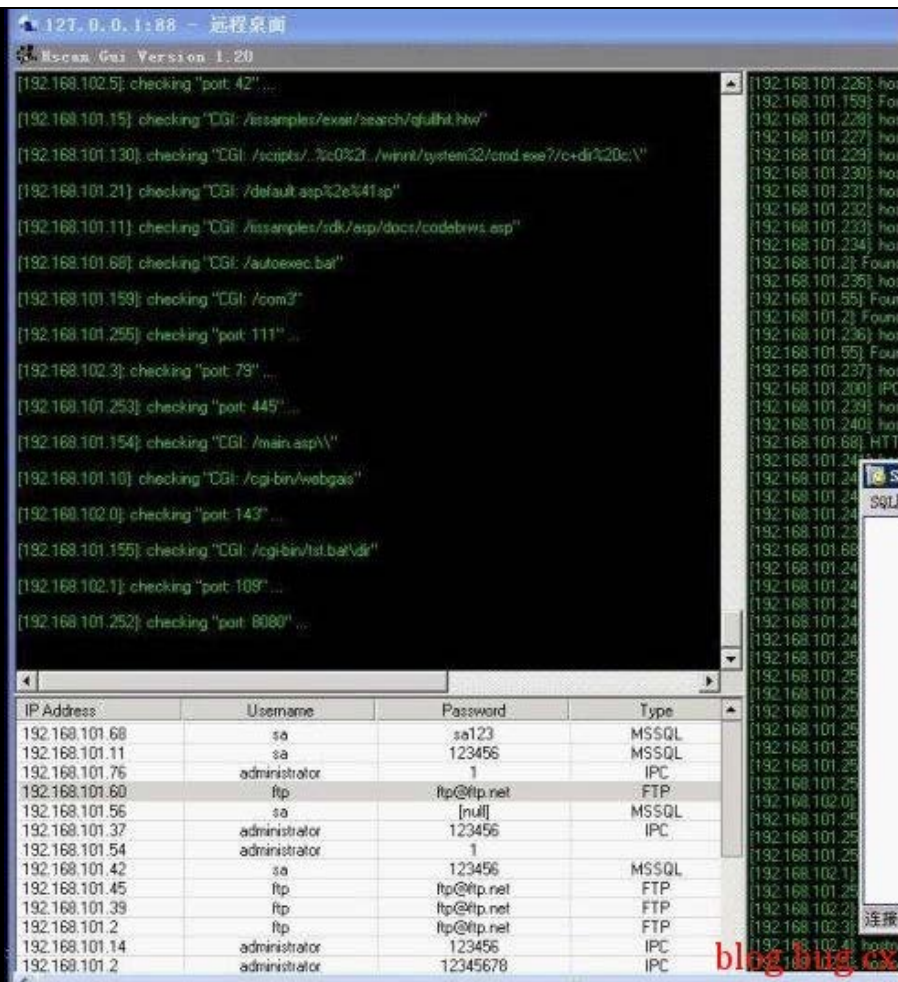


2.5 运用社会工程学以及密码习惯字典进行扫描收集管理信息

比如运用net group "domain admins" /domain net localgroup administrators这些命令找到DC管理并 破解密码 遇到这样的域我首先想到的是如何找到技术人员和运维技术的计算机，这些计算机有可能保存这这个内网众多的敏感信息。查看TCP以及端口连接信息，记录那些IP与当前的数据库服务器的数据库端口进行连接以及其他的服务器软件连接信息然后进行进一步渗透。可以使用XSCAN（使用nessus nasl脚本更新X-Scan漏洞库）或者俄罗斯商用SSS扫描器对内网做一个完全的安全扫描 收集管理密码,数据库账户密码,Web后台管理密码,硬盘内留下的以往的各类密码，分析管理员使用密码的习惯以及组合方式,组合密码字典扫描C类地址。查看IE缓存留下的Cookie信息，验证管理员留下的连接其他终端留下的痕迹是否有效，并记录,以便组合成针对目标网络的字典,如发现管理留下的连接其他服务器远程桌面的痕迹，验证并尝试 用当前主机密码登录,如失败，我留下一键盘记录器，如下图，支持ASP空间收信。

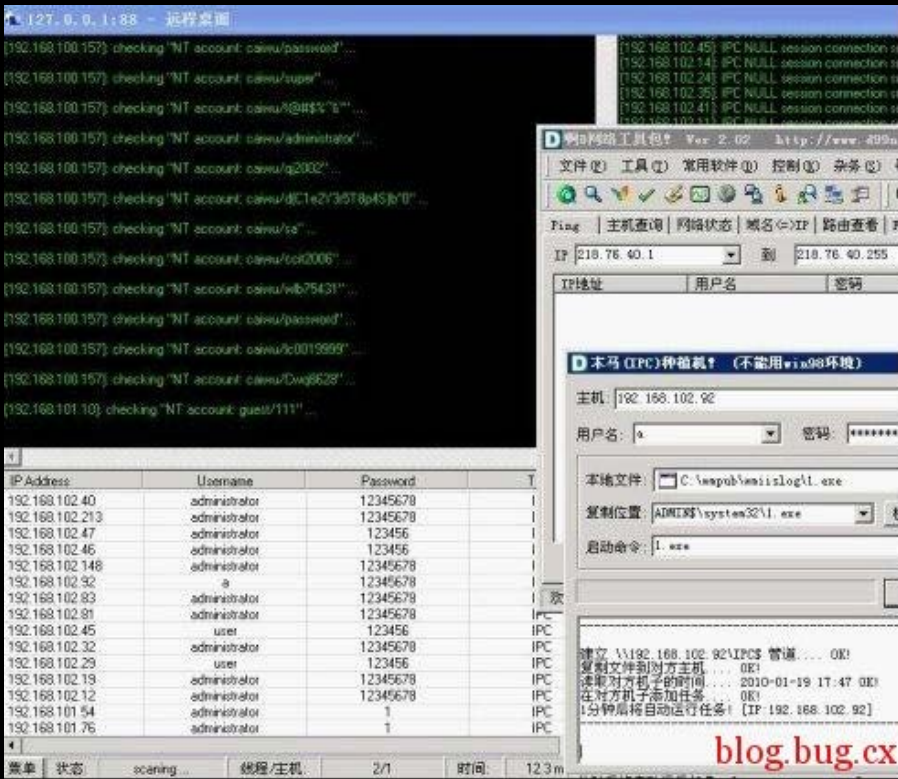


分析管理登录日志，以便及时获取管理信息,或者安装其他内核级的键盘记录器以便获取管理使用的其他密码，方便渗透。组合字典进行C类扫描，如图



2.4 内网常用的IPC\$共享入侵

IPC\$共享入侵时渗透公司企业内网一个比较快速的途径，（这也是企业内部员工密码安全意识薄弱的弱点）为了增快渗透速度我决定放弃手工而选用图形界面化的工具，结合上一步扫描，在上一步扫描为了避免扫描器过多占用系统资源导致当前主机不稳定的情况，在选择扫描模式和线程上注意调整，适应当前主机的承载能力，如图，进行的IPC\$共享以及弱口令扫描利用



在以上步骤上为了方便我采用为存在漏洞的机器植入反弹木马

上线名称	计算机名称	IP地址	操作系统	上线时间
渗透案例	CCIT-DATA01	202.111.1.252	Windows Server 2003	2010-1-19 15:58
渗透案例	ERPSQL2005-2	219.141.9.172	Windows Server 2003	2010-1-19 15:58
渗透案例	CYTS-VZ	202.111.1.252	Windows Server 2003	2010-1-19 15:58

2.5 ARP探嗅以及ARP挂马突破员工PC.

由于目标ARP设置存在安全缺陷，导致可以使用ARP探嗅和欺骗得到敏感数据以及网页挂马我们选择的是该目标内网员工的ERP办公系统。在这次探嗅中我选 用了两种大白鲨和cain （大白鲨截图丢失）如图

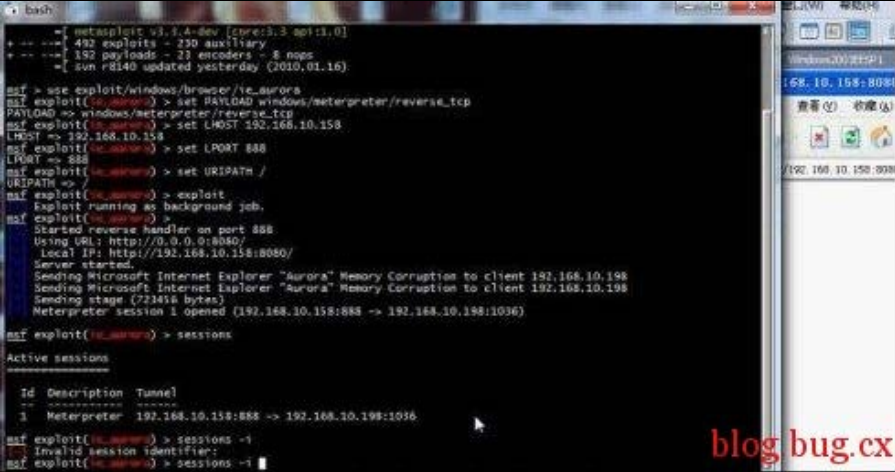


网页木马选择的是2010-01-17发布的IE漏洞EXP。 成功获取到部分员工Windows XP权限

渗透案例	KANGWEN	202.111.1.252	Windows XP Professional
渗透案例	LIJAMENG	202.111.1.252	Windows XP Professional
渗透案例	WANGZH	202.111.1.252	Windows XP Professional
渗透案例	CYTS-TT	202.111.1.252	Windows XP Professional

2.6 ERP内部员工办公系统挂马（Internet Explorer Aurora Exploit 2010-01-17）利用

在某些时候ARP挂马不一定生效，既然有了内部员工ERP办公WEB的权限那我就试试最新公布的Internet Explorer Aurora Exploit 为了规避风险问题，我决定在本地测试Internet Explorer Aurora Exploit 的稳定性，保证代码不造成目标员工PC电脑IE崩溃或者是程序异常（员工PC电脑的浏览器版本是在IPC\$获取员工权限后查看所得） 以下是部分测试截图，目前metasploit3.34已经更新了EXP。



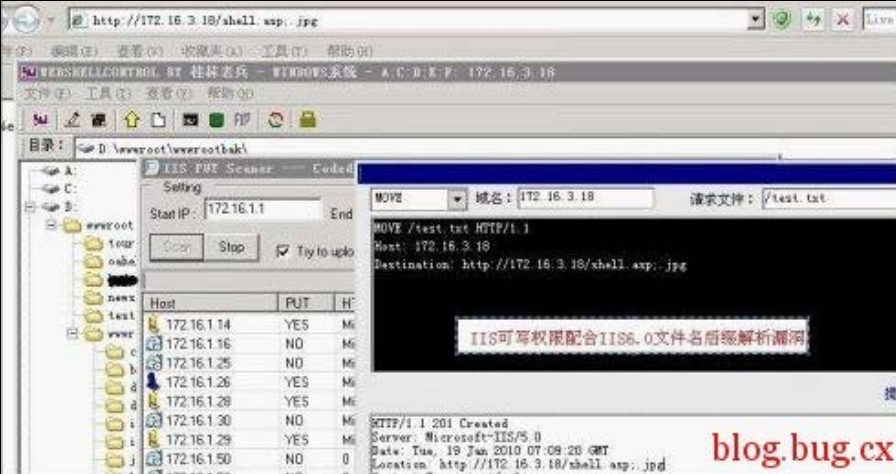


2.7 利用同步数据软件进行渗透

很多企业内网都安装了为数据提供同步的软件，但是安全配置上的失误导致入侵者可以通过这个将渗透 木马病毒延伸到各个角落，利用文件数据同步软件进行渗透的思路就是在同步的数据或者文件中篡改或者添加可以获得SHELL的文件如，Web asp PHP木马或者其他的补丁程序。（由于当时的图片已经丢失，就不做具体说明了）

2.8 利用IIS可写权限配合IIS6.0文件后缀名解析漏洞进行突破.

在2009年初IIS6.0就被公布出了存在文件后缀名解析漏洞，格式为x.asp; .jpg，很多的IIS6.0可写权限都是put到目标可以move 成Web Shell的时候出现失败的问题，我细心测试后发现可以结合这两个鸡肋做点文章。那就是move后缀时候用x.asp; .jpg来实现.如图。IIS权限 和安全配置失误一直是很多粗心大意的管理容易犯的问题



成功得到Web Shell 然后通过查看网站数据库配置信息来继续收集目标账户密码信息。

2.9 利用Windows XP 2K远程,local Exploits,溢出进行权限获取和提升

在上一步骤渗透得到一Web Shell，发现本机没有安装麦咖啡杀毒软件没有安装可供提升权限的第三方软件，通过systeminfo查看目标补丁信息如图

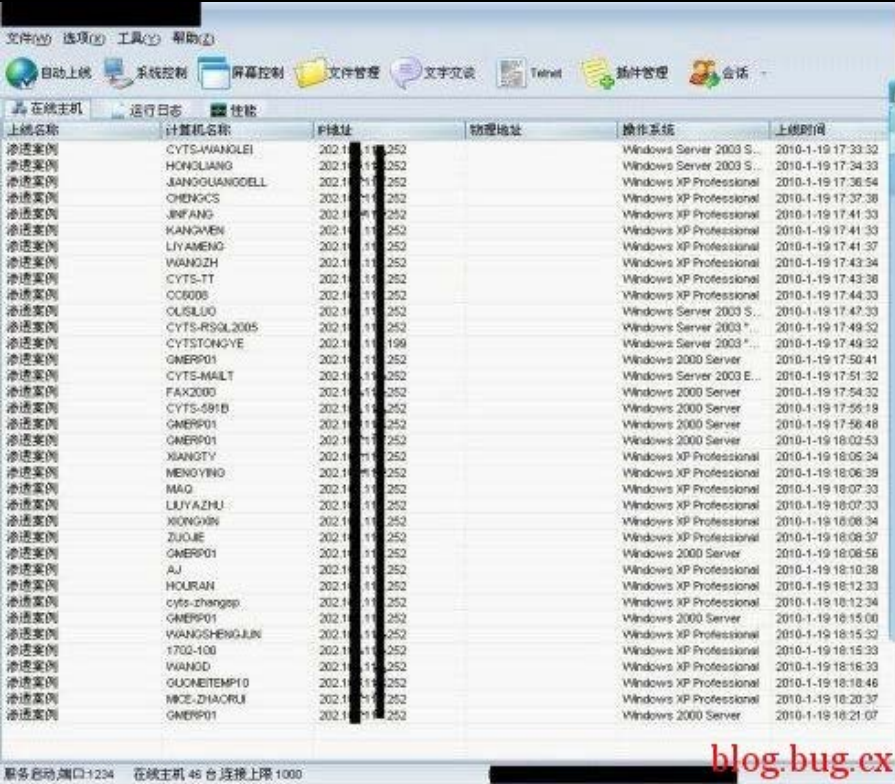


我通过Churrasco.exe来提权.这个loacl Exploits是2008-06发布的，相比之下成功率较高也可以利用一些新的系统 软件漏洞进行权限提升针对这个系统我只找到这个可以提升权限成功如图

```
C:\Inetpub\wwwroot>Churrasco.exe "ohoni"
/churrasco/-->Current User: Administrator
/churrasco/-->Process is not running under NETWORK SERVICE account!
/churrasco/-->Getting NETWORK SERVICE token ...
/churrasco/-->Found NETWORK SERVICE token 0x6c4
/churrasco/-->Getting Rpcss PID ...
/churrasco/-->Found Rpcss PID: 688
/churrasco/-->Searching for Rpcss threads ...
/churrasco/-->Found Thread: 692
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 696
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 704
/churrasco/-->Thread impersonating, got NETWORK SERVICE Token: 0x670
/churrasco/-->Getting SYSTEM token from Rpcss Service...
/churrasco/-->Found NETWORK SERVICE Token
/churrasco/-->Found LOCAL SERVICE Token
/churrasco/-->Found SYSTEM token 0x668
/churrasco/-->Running command with SYSTEM Token...
/churrasco/-->Couldn't run command, try again!
```

blog.bug.cx

2.9 以上方法配合反弹远程控制木马配合。
以上各类渗透手法的目的是获取权限，为了方便我使用远程控制软件，IPC\$植入反弹木马MSSQL连接上传植入木马执行.local Exploits 提权执行反弹木马都是可以的（我不赞成使用黑客工具，这次渗透式经过对方允许使用此类软件.这些软件会在对方系统植入档案改变设定.完成之后已经彻底清除 卸载恢复）
在这次渗透中共获取计算机权限52个，这其中达到了我们渗透的目标，内部员工办公PC，客户数据库等等，公司内部部的MAIL邮箱对付一个企业的发展来说做 必要的渗透测试并对系统，数据加固是很重要的，部分如图：



名称	计算机名称	IP地址	物理地址	操作系统	上线时间
渗透案例	CYTS-WANJIEI	202.103.110.252		Windows Server 2003 S...	2010-1-19 17:33:32
渗透案例	HONGJIANG	202.103.110.252		Windows Server 2003 S...	2010-1-19 17:34:33
渗透案例	JIANGGUANGDELL	202.103.110.252		Windows XP Professional	2010-1-19 17:36:54
渗透案例	CHENGCS	202.103.110.202		Windows XP Professional	2010-1-19 17:37:38
渗透案例	JIN FANG	202.103.110.252		Windows XP Professional	2010-1-19 17:41:33
渗透案例	KANGAVEN	202.103.110.252		Windows XP Professional	2010-1-19 17:41:33
渗透案例	LIYAMENG	202.103.110.252		Windows XP Professional	2010-1-19 17:41:37
渗透案例	WANGZHI	202.103.110.252		Windows XP Professional	2010-1-19 17:43:34
渗透案例	CYTS-TT	202.103.110.252		Windows XP Professional	2010-1-19 17:43:38
渗透案例	OC6008	202.103.110.252		Windows XP Professional	2010-1-19 17:44:33
渗透案例	OLISLUO	202.103.110.252		Windows Server 2003 S...	2010-1-19 17:47:33
渗透案例	CYTS-RSQL2005	202.103.110.252		Windows Server 2003 S...	2010-1-19 17:49:32
渗透案例	CYTSTON2VE	202.103.110.199		Windows Server 2003 S...	2010-1-19 17:49:32
渗透案例	GMERP01	202.103.110.252		Windows 2000 Server	2010-1-19 17:50:41
渗透案例	CYTS-MAILT	202.103.110.252		Windows Server 2003 E...	2010-1-19 17:51:32
渗透案例	FAK2000	202.103.110.252		Windows 2000 Server	2010-1-19 17:54:32
渗透案例	CYTS-591B	202.103.110.252		Windows 2000 Server	2010-1-19 17:55:18
渗透案例	GMERP01	202.103.110.252		Windows 2000 Server	2010-1-19 17:56:48
渗透案例	GMERP01	202.103.110.252		Windows 2000 Server	2010-1-19 18:02:53
渗透案例	XIANGTY	202.103.110.252		Windows XP Professional	2010-1-19 18:05:34
渗透案例	MENGYING	202.103.110.252		Windows XP Professional	2010-1-19 18:06:38
渗透案例	MAQ	202.103.110.252		Windows XP Professional	2010-1-19 18:07:33
渗透案例	LIUYAZHU	202.103.110.252		Windows XP Professional	2010-1-19 18:07:33
渗透案例	XIONGXIN	202.103.110.252		Windows XP Professional	2010-1-19 18:08:34
渗透案例	ZUJIE	202.103.110.252		Windows XP Professional	2010-1-19 18:08:57
渗透案例	GMERP01	202.103.110.252		Windows 2000 Server	2010-1-19 18:08:58
渗透案例	AJ	202.103.110.252		Windows XP Professional	2010-1-19 18:10:38
渗透案例	HOURAN	202.103.110.252		Windows XP Professional	2010-1-19 18:12:33
渗透案例	cyts-zhangp	202.103.110.252		Windows XP Professional	2010-1-19 18:12:34
渗透案例	GMERP01	202.103.110.252		Windows 2000 Server	2010-1-19 18:15:00
渗透案例	WANGSHENGJUN	202.103.110.252		Windows XP Professional	2010-1-19 18:15:32
渗透案例	1702-100	202.103.110.252		Windows XP Professional	2010-1-19 18:15:33
渗透案例	WANGD	202.103.110.252		Windows XP Professional	2010-1-19 18:16:33
渗透案例	GUANTEMPI0	202.103.110.252		Windows XP Professional	2010-1-19 18:18:46
渗透案例	NICE-ZHACRLJ	202.103.110.252		Windows XP Professional	2010-1-19 18:20:37
渗透案例	GMERP01	202.103.110.252		Windows 2000 Server	2010-1-19 18:21:07

blog.bug.cx

Microsoft Excel - 2010年1-2月产品成本核算 (基本)

客户数据, 商业机密被164297于一个企业的数据危害不容小觑

10年1-2月份产品成本核算

NO	产品名称	计划人数	出团日期	航空公司	所接人数	机票价(含税)	地接价GTA	餐费	门票	签证费	领队	导游交人	成本	外委价
10	美国8天	28	2月13日	南航	20	5700	4900	1070	0	810	240	0	127	14980
11	法德瑞3国5天	36	2月16日	南航	25	6000	4000	1140	320	870	240	-500	129	13688
12	德法荷比4国8+1天	41	2月10日	南航	30	4200	2400	960	325	870	0	-500	872	10999
13	德法荷比4国8+1天	41	2月17日	南航	20	4200	3300	960	325	870	0	-500	915	10688
14	意大利+希腊11天	20	2月10日	土航	15	4200	3774	960	325	870	280	-300	1015	10688
合计		447												

net 信息服务 (IIS) 管理器

操作(A) 查看(V) 窗口(W) 帮助(H)

标识符	状态	主机头值	IP 地址	端
1	已停止		* 全部未分配 *	80
8351	正在运行	rd.4000000000.com	* 全部未分配 *	80
80003692	正在运行	mail.4000000000.com	* 全部未分配 *	80

文件(F) 编辑(E) 视图(V) 项目(P) 查询设计器(Q) 工具(T) 窗口(W) 社区(C) 帮助(H)

对象资源管理器

连接(C) > 表

权限获取之后不做进一步的商业数据获取

t_name	t_phone	t_company	t_dep
孙广琪	59113371	自由行事业部	产品中
屈然	59113323	自由行事业部	产品中
郑宁	59113656	营销总部	呼叫中心
曹丽霞	59113670	自由行事业部	运营中
刘欣	59113327	自由行事业部	管理
宋继红	59113675	自由行事业部	运营中
蔡春英	59113699	自由行事业部	运营中
张红	59113005	国际商务公司	国际商
张京宏	59113006	自由行事业部	管理
李晋谨	59113008	国际商务公司	国际商
汪斌	59113216	国际商务公司	航空
秦超晨	59113217	国际商务公司	航空
吕君	59113220	国际商务公司	航空
原群晓磊	59113233	国际商务公司	航空
	59113251	国际商务公司	航空

ERPSQL2005-... temp_member		ERPSQL2005-... mp_unsemail		对象
客人姓名	省	证件类型	证件号码	出生
周天赤	北	身份证	■	1970
徐天	北	护照	■	1982
王占明	北	身份证	■	1963
朱玲玲	北	身份证	■	1954
郝钢	北	护照	■	1973
曹德安	北	护照	■	1941
赵守文	北	身份证	■	1963
刘葳	北	身份证	■	1965
黄湘宁	北	身份证	■	1968
张汇	北	身份证	■	1973
施震	北	身份证	■	1949
韩正义	北	身份证	■	1960
迟晓辉	北	身份证	■	1979
包显忠	北	身份证	■	1934
张桂影	北	身份证	■	1954
刘莹	北	身份证	■	1978
陈燕珊	北	身份证	■	1948
龚轶	北	身份证	■	

获取权限后停止，不做进一步的商业数据获取

blog.bug.cx

在渗透测试完成之后，所以在过程中利用到的记录器以及工具反弹木马都已经删除，系统恢复原状.此次渗透中获取的一些商业信息已完全删除.

并提交报告于目标的网络管理员。

内网渗透案例(续)

目标系统的安全加固和安全问题和解决参考

3.1 访问控制

1. 防火墙访问控制策略配置不完善，没有完全发挥边界防护的作用，内网数据存在泄露到外网的可能。

解决办法：

根据业务和安全需求调整访问控制策略，去掉冗余的规则，做到最小化原则。如细化防火墙对应用服务区域的访问控制策略等。

2. 没有修改网络设备的默认口令，可能造成非授权人员的访问。

解决办法：

设置一个足够复杂的强口令并定期更换，同时在交换机上做访问控制规则，对登录设备的IP进行限制。

3. 防火墙的管理仅使用一个超级用户。

解决办法：

根据业务需求，重新分配用户和权限，做到权责分明。

4. 操作系统帐号/口令策略采用默认设置

解决办法：

加强帐号/口令策略安全配置，增强当前服务器用户口令强度，并加强对特权用户远程登录的控制和管理，使用SSH加密方式对服务器进行远程管理，以防用户/口令信息泄露。

员工密码安全意识薄弱，可以对员工进行安全培训

5. 目标系统管理员访问控制存在安全隐患

解决办法：

管理员（内部员工）访问目标系统应设定严格的访问控制措施，如基于IP地址，MAC，只允许管理员（内部员工）在设定的IP地址对系统进行操作，避免因管理员（内部员工）帐户/密码泄漏给系统带来的威胁。

3.1 电信和网络安全

6. 防火墙没有启用足够的抗攻击等防护功能

解决办法：

启用防火墙必要的抗攻击功能。

1、可在根据日志审计的统计数据辅助设置开启抗攻击功能的阈值,FW上每个访问控制规则的日志也要接入，但防火墙抗网络攻击的能力和范围有限。

2.或者在防火墙前面架设电信级IPS，可抵御大部分网络攻击和拒绝服务攻击

3.2安全管理与实践

7. 部分设备还没有开启日志审计功能，使得潜在的攻击事件不具备追溯性

解决办法：

尽快部署专业日志审计服务器实现对设备日志的收集、存放和审计。

8. 互联网区没有划分安全域

解决办法：

启用核心交换机第三层功能，根据业务需求划分VLAN，并在VLAN之间实施适当的访问控制。

1. 在交换机上根据业务类型或者功能划分VLAN，可缓解业务高峰时的网络风暴的威胁，但须事先做好路由规划

2. 在各个安全域边界架设网络防火墙来防止因单一安全区域的蠕虫木马的扩散。

3. 在交换机上启用IP策略设定和禁止内部访问外部陌生地址。

3.3应用和系统开发安全

9. 操作系统没有关闭默认启动的冗余服务

解决办法：
根据业务需要，只开启必须的服务，关闭冗余的服务。避免冗余服务所带来的安全隐患

10. 数据库监听器配置

解决办法：
修改监听器配置，为监听器配置口令，这样对监听器进行操作时必须先输入口令进行认证；修改监听器配置参数，将“ADMIN_RESTRICTIONS”设为“ON”，这样在监听器运行时将禁止通过命令对监听器进行任何修改，必须手动修改监听器配置文件listener.ora才可以对监听器配置进行修改。

11. 数据库当前没有启用审计

解决办法：
启用数据库的审计功能或者部署专业的数据库审计系统对数据库系统管理、安全管理、数据维护、用户登录等事件进行审计，并由专人负责数据库的审计管理。
为了避免数据库开启监听功能后带来的性能问题，可以部署数据库安全审计设备。

12. 管理服务器存在高风险漏洞

解决办法
对用于集中对应用服务器和数据库服务器进行远程管理的PC服务器安装最新的安全补丁。

1. 在网络中架设补丁分发管理系统

2. 在网络中架设漏洞扫描器，可及时了解网络中的设备的漏洞情况

3. 对麦咖啡企业级防火软件设定管理密码，防止他人更改安全设置

13. 目标系统登录密码安全策略控制不严

解决办法
此次目标系统中应提高密码复杂度的要求，对用户密码进行检查，以提高用户密码的安全级别，如必须是数字和字母的组合等；定义可尝试输入密码的次数和对尝试输入密码采取相应安全策略，如连续输入3次错误密码，将锁定用户一小时等，防止恶意人员对用户的密码暴力破解。

14. 目标WEB系统异常输入检验机制存在缺陷

解决办法
根据实际情况对输入参数进行严格检查，包括输入字符的长度、类型，并对一些特殊字符进行过滤。在WEB服务器前面架设WEB应用防火墙可以定义非法字符的过滤策略。

15. 交换机使用默认的SNMP连接串

解决办法
设置一个具备一定复杂度的SNMP连接串。

1. 在交换机上修改。命令参考：
Router(config)#snmp-server community public/private RO

2. 在网络中架设漏洞扫描器可以检测出该漏洞

3.4加密

16. 目标系统的通信未采取加密措施

解决办法
对目标WEB数据传输进行加密，如采用https方式。更高安全级别考虑，建议考虑使用SSL vpn或HTTPS解决方案。

一. 目标系统安全加固解决办法总结
渗透测试发现的问题中，大多数是可以通过对现有的网络设备、安全设备、WEB数据库、WEB服务器、中间件等进行配置优化调节来解决的。但是仍然有几个问题是无法通过现有网络资源解决的，我们总结了一下大概有以下三点：
加密：可以对目标的数据传输进行加密
应用与系统安全：目标WEB系统异常输入检验机制
应用与系统安全：数据库安全审计

3.1 加密
目前解决目标数据传输进行加密有两种办法：
在WEB应用系统软件上面开启HTTPS传输功能。
HTTPS是以安全为目标的HTTP通道，简单讲是HTTP的安全版。它的主要作用可以分为两种：一种是建立一个信息安全通道，来保证数据传输的安全；另一种就是确认网站的真实性。HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议要比http协议安全。
但是我认为在WEB应用软件上面开启这项功能并不适用目标的员工办公系统以及为客户提供服务的系统。因为HTTPS服务器是需要对传输的数据加密和解压的，大规模的部署势必会严重影响WEB服务器的运行性能，最终导致服务器拒绝服务。
在WEB应用服务器前架设 SSL VPN加速器。

总结
古话说的好“堡垒最容易从内部突破”此次渗透案例正是诠释了这句话的。
分析管理登录日志，以便及时获取管理信息.或者安装其他内核级的键盘记录器以便获取管理使用的其他密码，方便渗透. 组合字典进行C类扫描

最新文章

相关文章

热评文章

Waiting

Waiting

webhack入侵思路及上传漏洞
MSSQL备份导出Shell中文路径解决办法

[nmap smb script](#)
[MS12-027 poc逆向分析](#)
[Linux流量监控工具 – iftop \(最全面的iftop教程\)](#)