项目 3

手工入侵共享连接主机

3.1 项目描述

IPC$是微软提供的一个“易用性”的功能，但是降低了系统“安全性”。本案例是针对操作系统存在IPC$“易用性”的攻击，学习本案例也促使用户在“易用性、安全性”之间进行正确的选择。

空连接就是不用密码和用户名的IPC$连接，在Windows下，它是用net命令来实现的。由空连接产生的会话的权限比较低，这种非信任会话并没有多大的用处，但从一次完整的IPC$入侵来看，空会话是一个不可缺少的跳板，因为可以从它那里得到用户列表，而大多数弱口令扫描工具就是利用这个用户列表来进行口令猜解的，成功导出用户列表可以增加密码猜解的成功率，仅从这一点就足以说明空会话所带来的安全隐患。

本案例假设已经得到密码为空的管理员账号，利用IPC$管道操作，向目标系统进行“传文件、远程开TELNET服务、添用户、安装特洛伊木马、开3389端口、清除日志”等操作，展示一个较为完整的入侵、加固、清除脚印的过程。

本案例使用ROTS.vbs脚本开3389端口。

3.2 漏洞描述

1. IPC$ 简述

IPC$(Internet Process Connection)是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。IPC$是Windows系统的一项功能，它有一个特点，即在同一时间内，两个IP地址之间只允许建立一个连接。Windows系统在提供了IPC$功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑共享(c$、d$、e$……)和系统目录winnt或Windows(admin$)共享。所有的这些，微软的初衷都是为了方便管理员的管理。在默认安全设置下，对于Windows系统，借助空连接可以列举目标主机上的用户和共享，访问Everyone权限的共享，访问小部分注册表等，虽然没有太大的利用价值，但导致了系统安全性的降低。

2. InstGina.exe

Gina木马的主要作用是，在系统用户登录时，将用户登录的名字、登录密码等记录到文

件中，因为这个 DLL 是在登录时加载的，所以不存在像 findpass 那类程序当用户名字是中文时，无法得到用户密码的情况。

网络上有很多这类的 Gina 木马存在，编写程序的原理都是一样的，常见的有 fakegina、win 2k 密码大盗、ntshell 等。

Gina 木马有两个程序，一个是 Gina. dll，一个是用于安装 DLL 木马的 InstGina. exe。

InstGina. exe 有三种用法。

(1) InstGina-view：这是查看系统中 GinaDLL 键值，判断是否有被安装过 DLL，主要用来查看系统是否被安装了 Gina 木马。

(2) InstGina-remove：这是将系统中 GinaDLL 键值删除，如果发现系统被安装了 Gina 木马，用于删除木马。

(3) InstGina-install：GinaDLL 文件名用于安装 Gina 木马。

安装方法如下。

(1) 将“InstGina. exe”和“Gina. dll”复制到同一个目录下，不要求一定要复制到 system32 目录下，因为 InstGina 如果发现当前目录不是系统目录，会将 Gina. dll 复制过去。

(2) 执行“InstGina. exe-install Gina. dll”命令，如果将 Gina. dll 重命名了，如改为 abc. dll，那么要执行的命令是“InstGina. exe-install abc. dll”。

(3) 看到“Set Gina Trojan Successfully”提示，证明安装成功，如果返回信息是“The Key GinaDLL Does Exist”，这证明 GinaDLL 键值已被设置，可以用-remove 将该键值删除，然后再安装。

记录保存到 wineggdrop. dat 中，类似程序还有可能加入其他的功能，例如：

(1) 用户登录时自动将一个自定义的账户加到 admin 组并设置密码(不会超过 30 行代码)。

(2) 定时将一个用户加入 admin 组并设置密码(上面的功能＋定时检查时间)。

3.3　项 目 分 解

整个项目可分为“传文件、远程开 TELNET 服务、添用户、安装特洛伊木马、开 3389 端口、清除日志”6 个部分，各个部分可以使用其他形式的方法实施。在现实的攻击中，根据具体的目标环境不同而加以变化。

传文件：使用 IPC＄建立连接，直接复制文件到目标系统。

远程开 TELNET 服务：远程开 TELNET 服务。

添用户：TELNET 到目标系统，添加用户。

安装特洛伊木马：入侵目标后，为系统添加登录木马 Gina，用于记录系统登录时的用户名和密码。

开 3389 端口：使用“ROTS. vbs”脚本为系统开 3389 端口。

清除日志：清除入侵过程留下的痕迹，本案例提供的方法较为粗糙，并没有细分要删除哪些内容，而是直接删除全部日志。

3.4 项目实训

1. 开启虚拟机

开启 Windows 2000 及 Windows XP 虚拟机，配置好虚拟机的网卡，设置为桥接模式，两台虚拟机可以 ping 通。在本项目中，虚拟机 IP 地址设置如下。

Windows 2000：192.168.0.100/255.255.255.0；管理员密码为空。

Windows XP：192.168.0.200/255.255.255.0。

假设攻击前已经通过扫描得到 Windows 2000 目标系统管理员用户密码为空。

2. 建立 IPC$ 连接

在 Windows XP 虚拟机中输入如下指令，建立 IPC$ 连接，如图 3-1 所示。

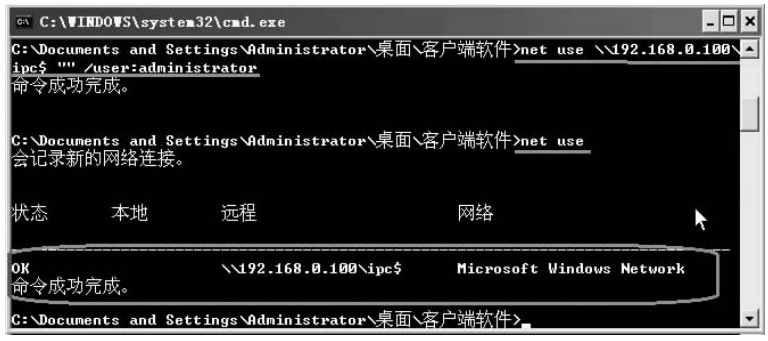

图 3-1

建立 Z 盘到 Windows 2000 admin$ 的映射，如图 3-2 所示。

图 3-2

3. 传送文件

使用 copy 指令直接将文件复制到 Z 盘，完成文件传送，如图 3-3 所示。

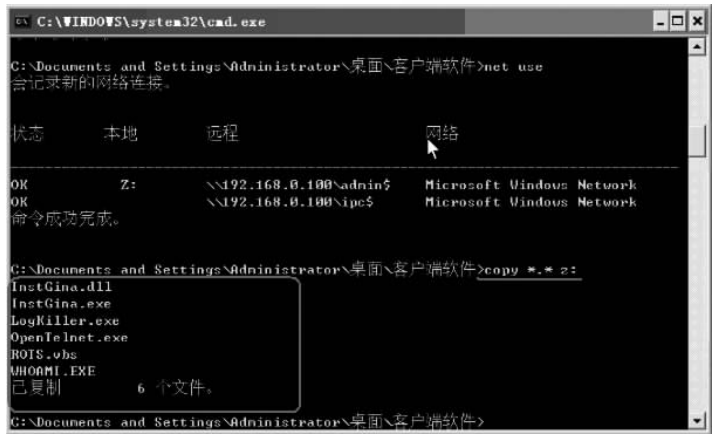

图　3-3

4. 远程开 TELNET 服务

OpenTelnet.exe 程序用于远程开 TELNET 服务，指令格式如下：

```
C:\Documents and Settings\Administrator\桌面\客户端软件>opentelnet
**********************************************************
Remote Telnet Configure,by refdom
Email: refdom@ 263.net
opentelnet
Usage:OpenTelnet.exe \\server username password NTLMAuthor telnetport
**********************************************************
```

OpenTelnet.exe　\\目标地址　用户名　密码　NTLM 认证方式　telnet 端口

NTLM 认证基于“提问—答复”机制对客户端进行验证。

NTLM 是 NT LAN Manager 的缩写。NTLM 是 Windows NT 早期版本的标准安全协议，Windows 2000 支持 NTLM 是为了保持向后兼容。Windows 2000 内置三种基本安全协议之一。

NTLM 工作流程如下。

(1) 客户端首先在本地加密当前用户的密码成为密码散列。

(2) 客户端向服务器端发送自己的账号，这个账号是没有经过加密的，明文直接传输。

(3) 服务器端产生一个 64 位的随机数字发送给客户端，作为一个 challenge(挑战)。

(4) 客户端再用加密后的密码散列来加密这个 challenge，然后把加密后的 challenge 作为 response(响应)，返回给服务器端。

(5) 服务器端把用户名、给客户端的 challenge、客户端返回的 response 这三个文件发送给域控制器。

(6) 域控制器用收到的用户名在 SAM 密码管理库中找到该用户的密码散列，然后使用该密码散列加密 challenge。

(7) 域控制器比较两次加密的结果，如果一致，那么认证成功。

从上面的过程可以看出，NTLM 是以当前用户的身份向 Telnet 服务器发送登录请求的，而不是用自己的账户和密码登录。例如，家里的机器名为 A(本地机器)，登录的机器名为 B(远地机器)，在 A 上的账户是 ABC，密码是 1234，在 B 上的账户是 XYZ，密码是 5678，需要 Telnet 到 B 时，NTLM 将自动以当前用户的账户和密码作为登录的凭据来进行上面的

7 项操作，即用 ABC 和 1234，而并非用登录账户 XYZ 和 5678，且这些都是自动完成的。

NTLM 身份验证选项有以下三个值。

0：不使用 NTLM 身份验证，而是使用用户名/密码进行身份验证。

1：先尝试 NTLM 身份验证，如果失败，再使用账户和密码。

2：只使用 NTLM 身份验证。默认是 2。

为简便操作，通常设置为 0，即不使用 NTLM 认证。

在目标系统开启 TELNET 服务操作如图 3-4 所示。

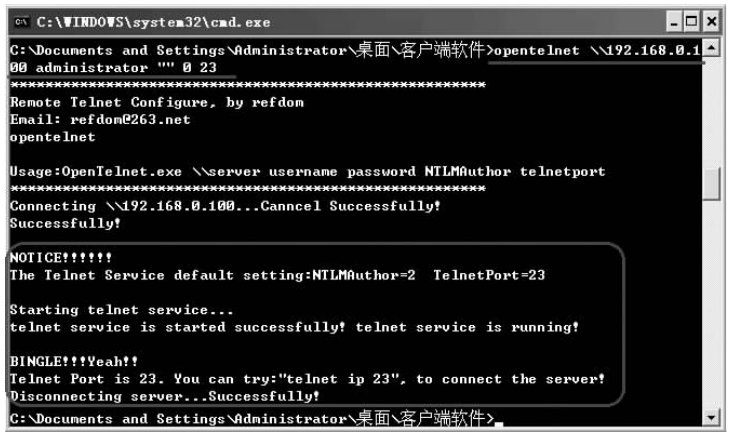

图 3-4

5. 添加用户

由于 Administrator 账户密码为空，可以不添加新用户。

更一般的做法还是为目标系统添加一个用户，并加入超级管理员组。

为目标系统添加“用户 a/密码 b”的操作为：

```
C:\Documents and Settings\Administrator>net user a b /add
```

命令成功完成。

“将用户 a 加入超级管理员组”的操作为：

```
C:\Documents and Settings\Administrator>net localgroup administrators a /add
```

命令成功完成。

6. 添加木马

为目标系统添加木马，用于窃取登录用户的密码。

在本案例中，既然已经取得管理员账户，而且添加了新用户 a，添加木马 Gina 不一定是必需的，在这里只作为一种攻击行为进行展示。

在前述步骤中，已经复制文件到目标系统的 Z 盘，所以，使用 cd 指令进入 Windows 系统目录，执行安装指令。

```
Instgina.exe    -install    instgina.dll
GinaDLL  Trojan  Installter  V1.0  By  WinEggDrop
Set  Gina  Trojan  Successfully
```

安装成功后，当用户登录时，账户及密码被记录到“wineggdrop. dat”文件，使用以下指令，可以查看“wineggdrop. dat”文件中的内容。

```
type  c:\winnt\system32\wineggdrop.dat
```

7. 开 3389 端口

ROTS. vbs——远程启动终端服务的 Windows 脚本。

特点：不依赖于目标的 IPC$ 开放与否。

原理：直接访问目标的 Windows 管理规范服务(WMI)。该服务为系统重要服务，默认启动。

支持平台：Windows 2000 Professional、Windows 2000 Server、Windows XP、Windows NT。

使用方法：在命令行方式下使用 Windows 自带的脚本宿主程序 cscript. exe 调用脚本，例如：

```
c:\>cscript ROTS.vbs <目标 IP 地址><用户名><密码>[服务端口] [自动重启选项]
```

服务端口：设置终端服务的服务端口。默认是 3389。

自动重启选项：使用/r 表示安装完成后自动重启目标使设置生效。使用此参数时，端口设置不能忽略。

脚本会判断目标系统类型，如果不是 Server 及以上版本，就会提示是否要取消。因为 Professional 版本不能安装终端服务。

在 Windows XP 虚拟机(注意：无须在 Windows 2000 的 TELNET 窗口)输入命令：

```
cscript  ROTS.vbs  \\192.168.0.100  administrator  ""  3389  /r
```

命令执行后如图 3-5 所示，目标系统重启。

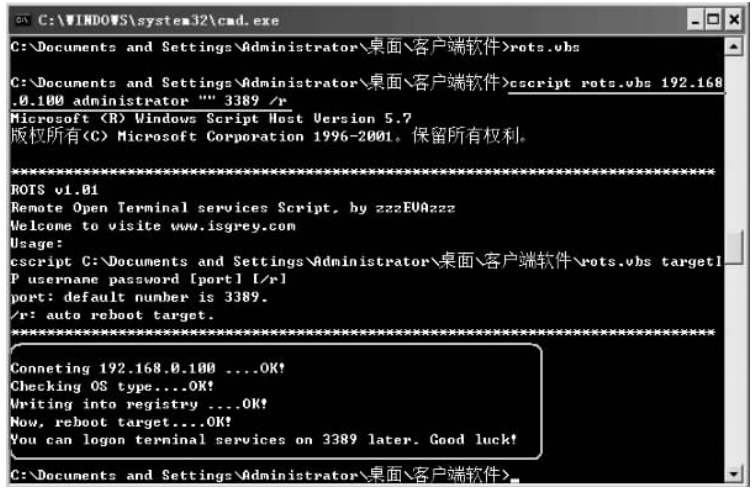

图　3-5

8. 远程桌面登录

等待目标系统完全启动后，在 Windows XP 系统打开“远程桌面连接”程序，输入目标系

统 IP 地址，单击“连接”按钮，出现目标登录界面，输入前面添加的“用户 a/密码 b”，可以成功登录到系统。

执行“whoami. exe”程序，可以查看当前登录用户信息，如图 3-6 所示。

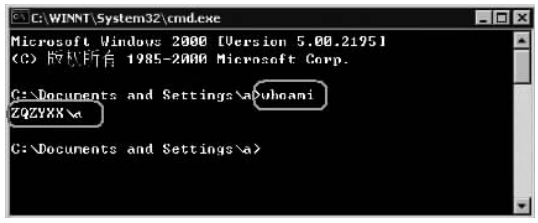

图 3-6

执行“type c:\winnt\system32\wineggdrop. dat”指令，显示木马记录的用户登录信息，如图 3-7 所示。

图 3-7

9. 清除入侵脚印

打开“事件查看器”窗口，可以分别查看“应用程序日志”、“安全日志”、“系统日志”3 种日志记录情况，如图 3-8 所示。

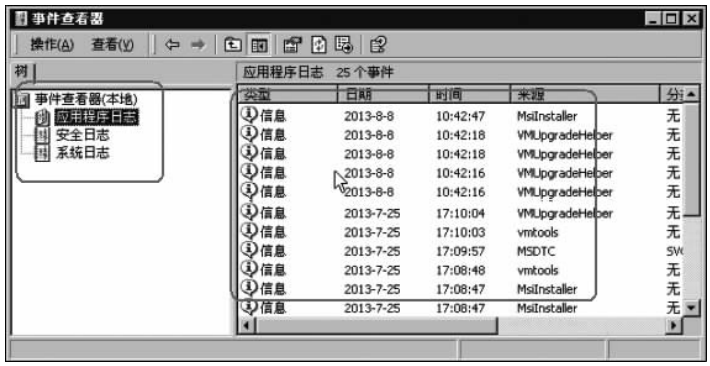

图 3-8

在命令行窗口执行程序“LogKiller.exe”，程序先停止日志服务，然后删除日志，最后重新启动日志服务。重新查看“事件查看器”窗口，发现所有日志已经被删除，如图 3-9 所示。

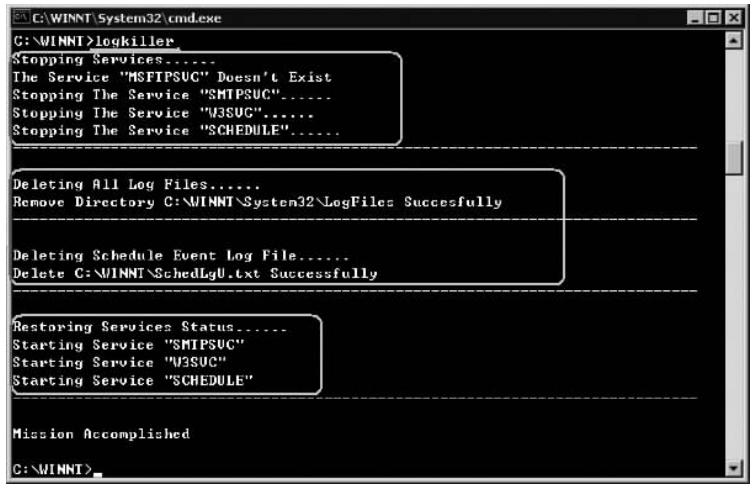

图　3-9

黑客入侵时，不需要在图形界面下清除日志，一般在得到字符界面时，就已经可以执行清除操作。本案例提供的方法较为粗糙，比较好的方法是，只删除与入侵者相关的日志条目，而非全部删除。这样操作会提高隐蔽性，不容易被发现。

3.5　项目小结

入侵空连接的方法多种多样，手法各不相同，本案例属于 IPC$ 经典入侵法。

本案例并没有借助溢出漏洞等技术，使用的方法由操作系统直接支持，大多数都是正常的操作。其中第一步建立 IPC$ 连接是关键，如果不能建立 IPC$ 连接，那么后边的操作就不能进行了，下面列举一些 IPC$ 连接失败的原因。

(1) 本机系统不是 Windows 操作系统。

(2) 对方没有打开 IPC$ 默认共享。

(3) 对方未开启 139 或 445 端口或被防火墙屏蔽。

(4) 命令输入有误，如缺少空格等。

(5) 用户名或密码错误，当然空连接是不需要密码的。

另外，也可以根据返回的错误号分析原因。

错误号 5，拒绝访问：很可能使用的用户没有管理员权限，先提升权限。

错误号 51，Windows 无法找到网络路径：网络有问题。

错误号 53，找不到网络路径：IP 地址错误；目标未开机；目标 lanmanserver 服务未启动；目标有防火墙(端口过滤)。

错误号 67，找不到网络名：本机 lanmanworkstation 服务未启动；目标删除了 IPC$。

错误号 1219，提供的凭据与已存在的凭据集冲突：已经和对方建立了一个 IPC$ 连接，应先删除原有的 IPC$ 连接后再连接。

错误号 1326，未知的用户名或错误密码。

错误号 1792，试图登录，但是网络登录服务没有启动：目标 NetLogon 服务未启动。连接域控制器会出现此情况。

错误号 2242，此用户的密码已经过期：目标有账号策略，强制要求定期更改密码。

3.6 知识链接

1. 安全连接建立过程

Windows NT 4.0 以后的系统是使用挑战响应协议与远程机器建立会话的，成功建立的会话将成为一个安全隧道，建立双方通过它互通信息，这个过程的大致顺序如下。

(1) 会话请求者(客户)向会话接收者(服务器)传送一个数据包，请求安全隧道的建立。

(2) 服务器产生一个随机的 64 位数(实现挑战)传送回客户。

(3) 客户取得这个由服务器产生的 64 位数，用试图建立会话的账号的口令加密，将结果返回到服务器(实现响应)。

(4) 服务器接收响应后发送给本地安全验证(LSA)，LSA 通过使用该用户正确的口令来核实响应以便确认请求者身份。如果请求者的账号是服务器的本地账号，核实过程在本地进行；如果请求者的账号是一个域的账号，响应传送到域控制器去核实。当对挑战的响应核实为正确后，产生一个访问令牌，然后传送给客户。客户使用这个访问令牌连接到服务器上的资源直到建立的会话被终止。

2. 空连接

空连接是在没有信任的情况下与服务器建立的会话(即未提供用户名与密码)，但根据 Windows 2000 的访问控制模型，空会话的建立同样需要提供一个令牌，可是空会话在建立过程中并没有经过用户信息的认证，所以这个令牌中不包含用户信息，但这并不表示空会话的令牌中不包含安全标识符 SID(它标识了用户和所属组)，对于一个空会话，LSA 提供的令牌的 SID 是 S-1-5-7，这就是空会话的 SID，用户名是：ANONYMOUS LOGON，这个用户名可以在用户列表中查看，但是不能在 SAM 数据库中找到，因为它属于系统内置的账号。在安全策略的限制下，这个空会话将被授权访问，Everyone、Network 这两个组有权访问到的一切信息。

3. 如何防范 IPC$ 入侵

如何防范 IPC$ 入侵？可以在以下 5 个方面对系统进行加固。

(1) 禁止空连接进行枚举

运行 regedit.exe，找到如下主键[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]，把 RestrictAnonymous=DWORD 的键值改为 1。

如果设置为“1”，一个匿名用户仍然可以连接到 IPC$ 共享，但无法通过这个连接得到列举 SAM 账号和共享信息的权限；在 Windows 2000 中增加了“2”，未取得匿名权的用户将不能进行 IPC$ 空连接。建议设置为 1。如果上面所说的主键不存在，就新建一个键值。如果觉得修改注册表麻烦，可以在“本地安全设置”窗口中设置此项：选择“本地策略”→“安全”→“对匿名连接的额外限制”命令。

(2) 禁止默认共享

① 查看本地共享资源。

选择“运行”命令,输入 cmd,在命令窗口中输入 net share。

② 删除共享(重启后默认共享仍然存在)。

net share ipc$ /delete

net share admin$ /delete

net share c$ /delete

net share d$ /delete(如果有 e、f、…可以继续删除)

③ 停止 server 服务。

net stop server /y (系统重新启动后 server 服务会重新开启)

④ 禁止自动打开默认共享(此操作并不能关闭 IPC$共享)。

选择“运行”命令,输入 regedit。

Server 版:找到如下主键。

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

把 AutoShareServer(DWORD)的键值改为 00000000。

Professional 版:找到如下主键。

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

把 AutoShareWks(DWORD)的键值改为 00000000。

这两个键值在默认情况下在主机上是不存在的,需要自己手动添加,修改后重启机器使设置生效。

(3) 关闭 IPC$和默认共享依赖的服务

通过禁止 server 服务,可以实现关闭 IPC$共享,步骤如下。

选择“控制面板”→“管理工具”→“服务”命令,找到 server 服务,右击,选择“属性”→“常规”→“启动类型”命令,选择“已禁用”选项,这时可能会有提示:×××服务也会关闭,是否继续。因为还有一些次要的服务要依赖于 server 服务,单击“是”按钮,继续关闭服务。

(4) 屏蔽 139、445 端口

由于没有以上两个端口的支持是无法建立 IPC$连接的,因此屏蔽 139、445 端口同样可以阻止 IPC$入侵,可以通过以下 3 个步骤来屏蔽端口。

① 139 端口可以通过禁止 NBT 来屏蔽。

在“本地连接属性”对话框中选择“Internet 协议(TCP/IP)”选项,单击“属性”按钮,单击“高级”按钮,选择 WINS 选项卡,选择“禁用 TCP/IP 上的 NetBIOS”选项。

② 445 端口可以通过修改注册表来屏蔽。

添加一个键值。

Hive:HKEY_LOCAL_MACHINE

Key:System\Controlset\Services\NetBT\Parameters

Name:SMBDeviceEnabled

Type:REG_DWORD