渗透测试

1 渗透测试基础

1.1 七个阶段

- 前期交互阶段
- 情报搜集阶段
  - 信息收集阶段分为**主动信息收集和被动信息收集**
- 威胁建模阶段
- 漏洞分析阶段
- 渗透攻击阶段
- 后渗透攻击阶段
- 报告阶段

2 Kali Linux基础

基本命令：

Ls	显示文件或目录
mkdir	创建目录
cd	切换目录
touch	创建空文件
cat	查看文件内容
cp	拷贝
mv	移动或重命名
find	在文件系统中搜索某文件

系统管理命令：

stat	显示指定文件的详细信息，比ls更详细
who	显示在线登陆用户
whoami	显示当前操作用户
hostname	显示主机名
uname	显示系统信息
top	动态显示当前耗费资源最多进程信息
ps	显示瞬间进程状态 ps -aux
du	查看目录大小 du -h /home带有单位显示目录信息

df	查看磁盘大小 df -h 带有单位显示磁盘信息
ifconfig	查看网络情况
ping	测试网络连通
netstat	显示网络状态信息
man	命令不会用了？用man指令，如：man ls
clear	清屏
kill	杀死进程，可以先用ps 或 top命令查看进程的id，然后再用kill命令杀死进程。

软件包管理：

- dpkg 离线
- apt 在线

3 Metasploit框架

Metasploit是一个开源的渗透测试框架软件，也是一个逐步发展成熟的漏洞研究与渗透代码开发平台。

Meterpreter在后渗透攻击阶段提供了强大功能

Meterpreter可以看做一个支持多操作系统平台，可以仅仅驻留于内存中并具备免杀能力的高级后门工具

Metasploit框架中的exploits可以分为两类：**主动型与被动型。**

- 主动型：主动型exploits能够**直接连接并攻击特定主机**
- 被动型：被动型exploits则等待主机连接之后对其进行渗透攻击。被动型exploits常见于浏览器，FTP这样的客户端工具等，也可以用邮件发出去，等待连入。

常见命令：

- msf> search：**正则查询的功能。当你想要查找某个特定的渗透攻击、辅助或攻击载荷模块时，搜索**(search)**命令非常有用**。
- msf> show auxiliary：**这个命令会显示所有的辅助模块以及它们的用途**
- msf> show options：参数(options)是保证Measploit框架中各个模块正确运行所需的各种设置。
- msf> show payloads：**攻击载荷是针对特定平台的一段攻击代码，它将通过网络传送到攻击目标进行执行。**
- msf> use：找到攻击模块或者payloads后，可以使用use命令加载模块
- msf> show targets：Metasploit的渗透攻击模块通常可以列出受到漏洞影响目标系统的类型
- msf> info：用info命令加上模块的名字来显示此模块的详细信息、参数说明以及所有可用的目标操作系统
- msf> check：Check可以用于检测目标主机是否存在指定漏洞
- msf>set和unset：Metasploit模块中的所有参数只有两个状态：已设置(set)或未设置(unset)。使用set命令可以针对某个参数进行设置（同时启动该参数）；使用unset命令可以禁用相关参数。

4 被动信息收集

被动信息收集也就是说不会与目标服务器做直接的交互、在不被目标系统察觉的情况下，通过搜索引擎、社交媒体等方式对目标外围的信息进行收集

5 主动信息收集

主动信息收集和被动信息收集相反，主动收集会与目标系统有**直接的交互**，从而得到目标系统相关的一些情报信息。

步骤：发现主机，端口扫描，指纹探测，WEB指纹探测，WEB敏感目录扫描