一、什么是PWN

PWN是一个黑客之间使用的词语，通常指攻破设备或系统。发音类似“砰”，对黑客而言，这象征着成功实施黑客攻击的声音——砰的一声，被“黑”的电脑或手机就被操纵了。在网络安全语境中，PWN通常指的是通过不同的攻击手段如利用漏洞、进行社会工程学攻击等方法成功地获得了一个设备、系统或网络的未授权控制权。一旦攻击者“PWN了”一个系统，他们就可以执行各种恶意活动，如窃取数据、安装恶意软件或制造更广泛的破坏。

在CTF（Capture The Flag）等黑客竞赛中，PWN任务经常涉及在一个受限制的环境中寻找和利用漏洞来访问受保护的资源或系统。具体来说，PWN题目通常会提供一个用C或C++编写的程序，该程序运行在目标服务器上，参赛者需要通过网络与服务器进行交互，利用程序中的漏洞（如栈溢出、堆溢出、整数溢出、格式化字符串漏洞等）来造成内存破坏，进而获取远程计算机的shell，并最终获得flag。

二、常见PWN漏洞

```
栈溢出（Stack Overflow）
```

栈溢出是一种常见的安全漏洞，它利用了程序在执行过程中使用的栈内存空间有限的特性。栈是一种数据结构，用来存储函数的局部变量、函数的参数以及函数调用的返回地址等信息。栈的特点是先进后出，即最后进入栈的数据最先被访问到。当攻击者向程序输入过多的数据时，这些数据会超出栈内存所能容纳的范围，从而覆盖了栈中的其他数据，甚至覆盖了函数返回地址。一旦返回地址被篡改，程序就会跳转到攻击者指定的代码执行，从而实现任意代码执行的攻击。

```
堆溢出（Heap Overflow）
```

堆溢出是另一种内存溢出漏洞，但与栈溢出不同，它发生在程序的堆内存区域。堆是用来动态分配内存的区域，程序员可以请求分配任意大小的内存块，并在程序运行期间随时释放它们。堆溢出通常是由于程序在写入数据时超出了申请的内存块大小，导致数据覆盖了相邻的内存块。

```
整数溢出（Integer Overflow）
```

整数溢出发生在将一个较大的整数赋值给一个较小范围的整数变量时，导致数据超出该变量的存储范围并发生溢出。这种溢出可能导致数据被截断、覆盖或产生不正确的计算结果。攻击者可以利用整数溢出漏洞来绕过安全限制、绕过认证机制或执行其他恶意操作。

```
格式化字符串漏洞（Format String Vulnerability）
```

格式化字符串漏洞通常发生在C语言等编程语言中，当程序不正确地处理格式化字符串函数（如printf、sprintf等）的输入时。攻击者可以通过构造特制的格式化字符串来读取或写入任意内存地址的数据，甚至执行任意代码。

```
ROP（Return-oriented Programming）
```

ROP是一种利用程序中的现有代码片段（称为“gadgets”）来执行攻击者意图的技术。在启用了某些安全保护（如NX位、ASLR等）的环境中，传统的栈溢出攻击可能难以直接执行shellcode。ROP通过覆盖返回地址为程序中的某个gadget的地址，并利用一系列这样的gadgets来构建攻击载荷，最终实现攻击者的目标。

入门指南:

Ununtu安装

镜像下载：

阿里云: https://mirrors.aliyun.com/ubuntu-releases/

在虚拟机点击安装VMware Tools，会提示没有任何 VMware Tools 映像。

解决方法：sudo apt-get install open-vm-tools-desktop

nc

nc全称是netcat,是一个功能强大的网络工具，其功能是用于扫描与连接指定端口，有着网络界的瑞士军刀美称。nc命令可用于扫描网络中的主机端口，支持tcp和udp连接，对于网络工程师来讲，可以方便的进行网络问题的排查。
1.安装:

sudo apt update

sudo apt install netcat #ubuntu系统

sudo yum install nc #centos系统

链接：http://www.cppblog.com/zhangyq/archive/2024/04/22/230335.html

nc ip地址 ip端口

pwntools

Pwntools 是一个 CTF 框架和漏洞利用开发库。它使用 Python 编写，旨在快速进行原型设计和开发，并尽可能简化漏洞利用的编写。

链接：https://github.com/Gallopsled/pwntools

安装命令:

sudo apt-get update
sudo apt-get install python3 python3-pip python3-dev git libssl-dev libffi-dev build-essential
python3 -m pip install --upgrade pip
python3 -m pip install --upgrade pwntools

IDA pro

交互式反汇编器专业版（Interactive Disassembler Professional），人们常称其为IDA Pro，或简称为IDA。是最棒的一个静态反编译软件，为众多0day世界的成员和ShellCode安全分析人士不可缺少的利器。IDA Pro是一款交互式的，可编程的，可扩展的，多处理器的，交叉Windows或Linux WinCE MacOS平台主机来分析程序， 被公认为最好的花钱可以买到的逆向工程利器。IDA Pro已经成为事实上的分析敌意代码的标准并让其自身迅速成为攻击研究领域的重要工具。它支持数十种CPU指令集其中包括Intel x86，x64，MIPS，PowerPC，ARM，Z80，68000，c8051等等。

.so文件

共享对象文件（Shared Object file），是Linux/Unix系统中的动态链接库文件，相当于Windows中的DLL文件

.so文件（Shared Object file）是类Unix系统（如Linux、Android等）中使用的动态链接库文件，其功能类似于Windows系统中的DLL文件。