内网/外网

Ipconfig/all 10.\*.\*.\* 172.16. \*.\* 192.168.\*.\*这样的ip均为内网

ASDL用户

Nc –vv –l –p 80 nc –vv 外网ip 80如果可以连接上即为外网

代理技术：

HTTP代理：只能代理浏览器 浏览器—工具—选项----局域网设置（代理服务器上为lan使用代理服务器，然后写上代理的ip地址和代理端口）

ftp代理：代理客户机上的ftp服务器，端口一般为21

Telnet代理：能够代理telnet，用于远程登录，端口23

Socks代理：全能代理，支持多种协议

坚持写博客

学习----询问----反馈 简历使用word文档

Python

Linux shell编程

React native

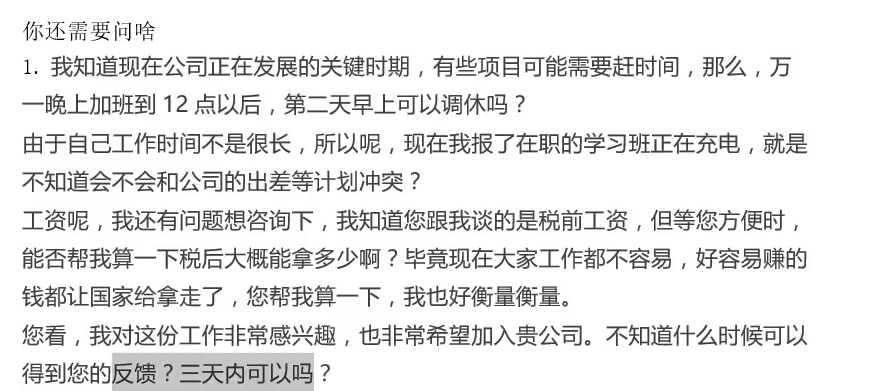
Web前端

数据库

黑客技术

CCIE

Vc++/java



PX是Pixel的缩写，也就是说像素是指基本原色素及其灰度的基本编码，由 Picture(图像) 和 Element（元素）这两个单词的字母所组成的，如同摄影的相片一样，数码影像也具有连续性的浓淡阶调 若把影像放大数倍，会发现这些连续色调其实是由许多色彩相近的小方点所组成，这些小方点就是构成影像的最小单位“像素”。这种最小的图形的单元能在屏幕上显示通常是单个的染色点。像素的大小是会“变”的，也称为“相对长度”。越高位的像素，其拥有的色板也就越丰富，越能表达颜色的真实感。[如大多数网页制作常用图片分辨率为72，即每英寸像素为72，1英寸等于2.54厘米。那么通过换算可以得出每厘米等于28像素，比如15\*15厘米长度的图片，等于420\*420像素的长度。

同时安装py2和py3的问题

1. 可以把同一个python.exe改个名字
2. 安装过程很简单，直接下载相应的包，点击安装
3. 如果需要分别运行不同的文件，则可以通过py -2/-3 ##.py 来运行不同的文件
4. 如安装不同的模块或库文件时，有 py -2/-3 setup.py install
5. 其他注意点需参考2版本和3版本之间的区别，如数据库使用（2：MySQLdb,3:pymysql）的不同等
6. 使用Pip： py -2/-3 –m pip install XXXXX(如django等)
7. 程序内可加 #！python2 或 #！python3 解析运行版本
8. #！python2
9. #coding:utf-8

肉鸡、后门、挂马

IPC$：共享“命名管道”的资源 ，为了进程间通信而开放的命名管道

弱口令

加壳：压缩体积或加密程序编码，甚至躲过杀毒软件查杀 UPX、UPack

花指令：颠倒病毒头脚，让杀毒软件找不到病毒

Ctrl+shift+Esc:任务管理器

21：FTP

25：SMTP

53: DNS

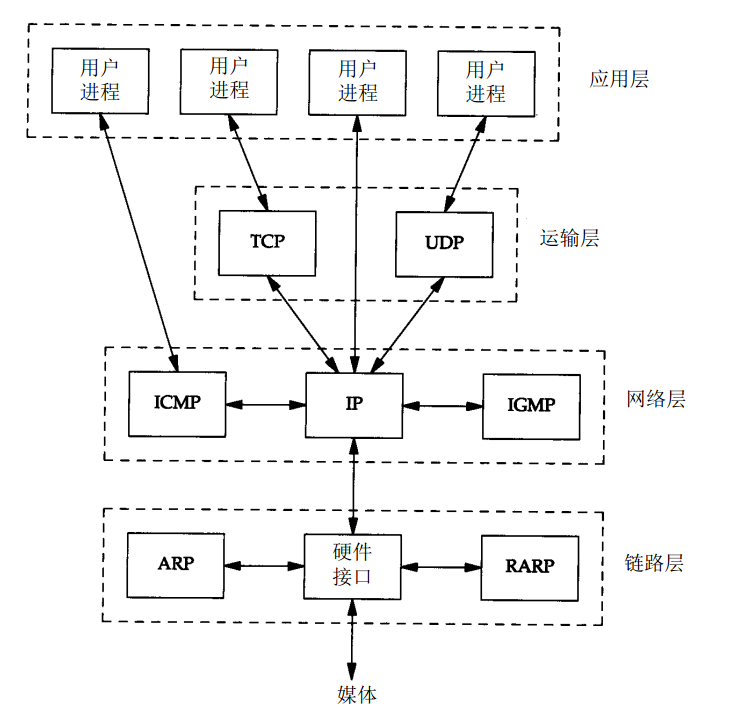
80: HTTP

110: POP3

3306: MySQL

3389: SQL

8080: Tomcat

 五类IP地址：

A 一个字节的网络地址和三个字节的主机地址1.0.0.1~126.255.255.254

B 两。。。。+两。。。。。。。。： 128.0.0.1~191.255.255.254

C： 三。。。。+一。。。。。。。。：192.0.0.1~223.255.255.254

D: 用于多点广播 ： 1110是第一个字节的开头 专门保留地址，并不指向特定的网络

224.0.0.1~239.255.255.254

E： 11110开头 为将来使用的保留 0.0.0.0：对应于当前主机 全1的IP地址（255.255.255.255）是当前子网的广播地址，地址范围是 240.0.0.1~255.255.255.254

常用的是 ABC三类，0.0.0.0：代表本网络

ping -t

netstat –a –n: 查看端口

netstat –a

Telnet :允许用户登录远程主机系统

telnet 192.27.2.130 80

利用QQ获得对方计算机的IP地址

选择通信的好友，他回复即可

他回复之后，cmd中输入 netstat -n 即可查看ESTABLISHED状态对应的外部IP地址，该地址为目标主机的IP地址



ProtectX 追踪软件

Regedit:

禁止匿名用户对命名管道IPC$的访问

展开： HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 将 restricanonymous 值改为1. 禁止自动管理共享： HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters AutoShareServer 改为0.

认识常见脚本病毒及防范

自动重启病毒：

打开记事本，写入“shutdown /r”命令，保存为 名字.bat 文件，创建快捷方式（.link）右键属性，可以更改图标以迷惑对方，当点击运行的时候计算机会自动重启。

U盘病毒一般可隐藏，所以插入后有病毒提示但是文件中如果没显示，可以进行杀毒再使用。

VBS 病毒生成机器 以.vbs结尾的文件

如刷qq群脚本：

Set WshShell = Wscript.CreateObject ("Wscript.Shell")

Wshell.AppActive "这个群真好玩"

for i =1 to 10: //控制发送次数

WScript.sleep 500

WshShell.SendKeys "^v"

Wshell.SendKeysｉ

Wshell.SendKeys　＂％s＂

Next

//当需要运行脚本的时候。把文件的扩展名改为.vbs，打开一个群聊天界面后把需要发送的内容复制在

剪贴板上，双击刚修改的##.vbs文件切换到聊天窗口上，即可自动刷屏。

VBS病毒特点：

1. 绝大多数VBS脚本运行需要一个文件系统对象
2. 运行需要关联WScript.exe的支持
3. 通过网页传播的需要ActiveX的支持
4. 通过邮件发送的需要OE的自动发送邮件功能支持

防范VBS脚本病毒：

1. 禁用文件系统对象 regsvr32 scrrun.dll/u 禁止文件系统对象
2. 在windows目录下，找到WScript.exe 更改名称或者删除。
3. 将浏览器的ActiveX控件及插件的一切设置为禁用
4. 禁止OE的自动收发邮件功能。

宏病毒防范：

1判断：有提示宏病毒，设置宏病毒安全两次打开word不能连续保持有效

2方法：杀毒软件、将文件另存为写字板（RTF）或word格式

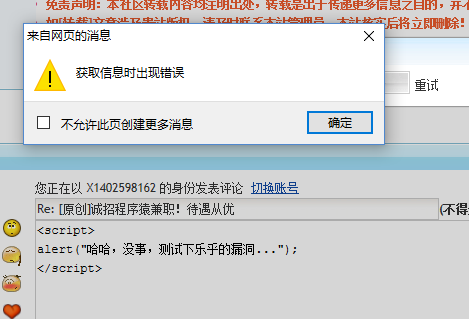
Linux抓包破解WiFi密码：

单击inidwep-gtk 选择加密方式 搜出热点 弹出新的窗口 选择字典 等待破解

SQL注入攻击： 用户可提交一段数据库查询代码，根据程序返回的结果，获得某些想知道的数据，国内的网站用 ASP+Access 或SQL Server占70%以上

Domain 注入工具

Cookies欺骗： 冒充别人登录论坛或网站 每台计算机都有确定的cookies值



黑客追踪工具： Neo TracePro

理解分布式计算和云计算的基本概念

参考书籍《分布式系统及云计算概论》 清华大学出版社

分布式系统是一组自治的计算机集合，通过通信网络相互连接，实现资源共享和协同工作，而呈现给用户的是单个完整的计算机系统。

1. 分布式计算系统
2. 分布式信息系统
3. 分布式普适系统

客户-服务器模式

客户-服务器也可以被理解为一个物理分布上的逻辑整体，它是由客户机、服务器和连接支持部分组成，通常所说的client-server端通信源于此。

客户-服务端架构和体系结构

1. 面向连接的服务
2. 无连接的服务

进程通信分为：

1. 并发服务器
2. 迭代服务器

该模型的进程通信协议

进程间通信是分布式系统的核心，由于没有共享存储器，分布式系统都是基于底层网络提供的底层消息传递机制的。这里主要

基于OSI（Open System Interconnection Reference Model,开放系统互连参考模型）参考模型而言的，这一参考模型可以分为7层：物理层、数据链路层、网络层、运输层、会话层、表示层和应用层，每一层一个模块，负责通信中特定的问题，并有自己的通信协议。

集群计算、网格计算、并行计算、云计算

1. 计算机集群简称为集群，它是一种计算机系统，通过将一组松散集成的计算机软件和硬件连接起来，高度协作完成计算工作。在某种意义上，它们可以被看成一台计算机，而每台计算机通常称为结点。集群有同构和异构之分。
2. 网格计算是利用大量异构的计算机的未用资源(如CPU周期和硬盘存储)，将其作为嵌入在分布是电信基础设施中的一个虚拟的计算机集群。网格计算的重心2放在跨区域计算管理能力上，这就是它与传统的计算机集群或传统的分布式计算的不同之处。
3. 并行计算是指同时使用多种计算机资源解决计算问题的过程。
4. 分布式计算是一门利用互联网的计算机中央处理器的闲置处理能力来解决大型计算问题的一门计算机科学，它研究如何将一个需要非常巨大的计算能力才能解决的问题分为许多小的部分，然后将这些小的部分分配给许多计算机进行并行处理，最后将这些计算结果综合起来得到最终的结果。
5. 云计算是分布式计算、并行计算的发展，或者说是这些计算机科学概念的商业实现。云计算技术使计算分布在大量的分布式计算机上，而不是本地计算机或远程服务器当中，其数据中心的运行将与互联网更加相似。这使得用户能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。在这里给出它的系统定义，云计算由一系列可以动态升级和被虚拟化的资源组成，这些资源被所有云计算的用户共享并且可以方便地通过网络访问，用户无需掌握云计算的技术，只需要按照个人或者团体的需要租赁云计算的服务。

WIFi网络的构成

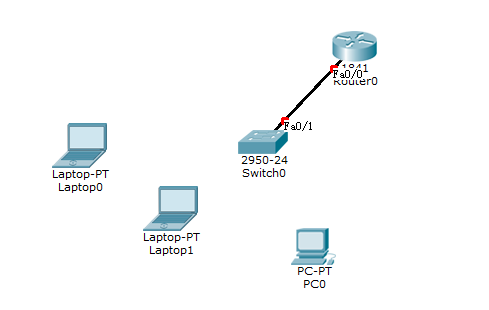
WIFI是一个无线网络通信技术的标准。网络按照区域分类分为局域网、城域网和广域网。无线网络是相对局域网而言的。一半架设WIFI网络的基本设备就是无线网卡和一台AP（无限访问接入点或桥接器），如无线路由器，它主要在媒体存取控制层MAC中扮演无线工作站和有限局域网络的桥梁。

WIFi工作原理：

WIFi设置至少需要一个Access Point（AP）和一个或一个以上的客户端。AP每100ms将SSID（Service Set Identifier）经由beacons（信号台）封包广播一次。beacons封包的传输速率是1 Mbit/s，长度相当的短，这个广播动作对于网络性能影响不大，因为WIFi规定的最低传输速率是1 Mbit/s，所以确保有的WIFi客户端都能接收到这一个SSID广播封包，客户端能够借此决定是否要和这一SSID的AP连线。

概念理解：

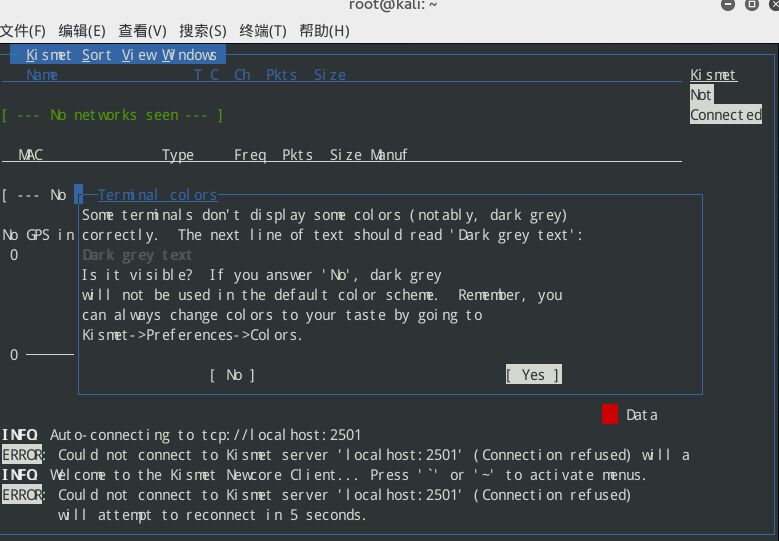
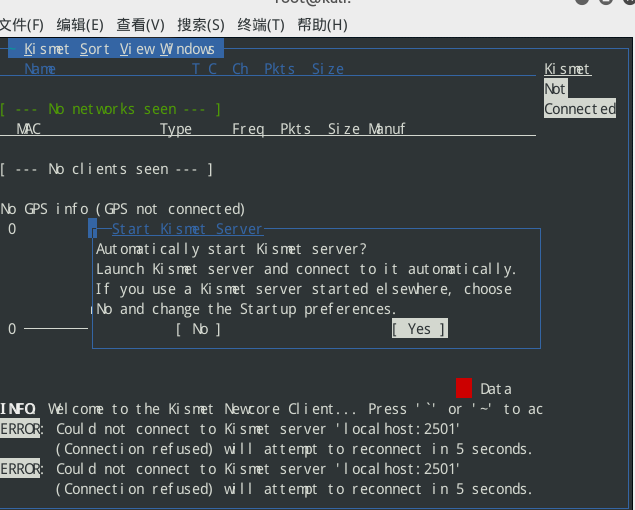
SSID：Service Set Identifier 的缩写，意思是服务集标。SSID技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权对的用户进入子网络。



WIFi拓扑结构

在Kali中使用Kismet 扫描无线网络

Kismet是一个图形界面的无线网络扫描工具，该工具通过测量周围的无线信号，可以扫描到附近所有可用的AP及所使用的信道。Kismet工具不仅可以对网络进行扫描，还可以捕获网络中的数据包到一个文件中。这样可以方便用户分析使用。下面是具体操作流程：

1. 在终端中输入命令：kismet 打开该工具。打开界面如下：
2.  start

151.101.24.133

[www.lvxingyu.xyz](http://www.lvxingyu.xyz)

<http://avatar.csdn.net/3/3/3/1_gane_cheng.jpg>

<https://github.com/xingyushu>

<http://blog.csdn.net/boke14122621>

manifest="http://www.ganecheng.tech/index.manifest"