加密,解密

GPG

对称加密

使用相同的密码加密解密

非对称加密

不同 , 公钥私钥

AIDE入侵检测

扫描与抓包

抓包: tcpdump

– tcpdump [选项] [过滤条件]

选项:

-i : 指定监控的网络接口

-A: 转换为ACSII码,

-w: 将数据包信息保存到指定文件(不会向屏幕再输出内容)

-r : 从指定文件读取数据包信息

-c : 定义抓包个数

过滤条件:

类型: host net port portrange

方向: src dst

协议: tcp udp ip wlan arp icmp

组合: and or not

注意:

or: 把第一个作为第一个条件

\(......)\

\: 转意符号

1 and \(2 or 3)\

1 and 2 or 3 //1,2作为

抓包工具

wireshark

wireshark-gnome

(Yum下载)

打开方式

]#wireshark

生产环境中一般用tcpdump去抓包的,

用tcpdump抓包,并存储在文件里,

再用wireshark打开文件分析