

1 GPG工具的主要功能及对应的防护目标是什么

参考答案

主要提供加解密、签名及校验功能：

- 1) 加密/解密：保证数据完整性，保证数据的机密性
- 2) 签名及校验：保证数据完整性，实现认证功能以及不可否认性

2 使用gpg工具实现非对称方式的加密/解密操作

用户bob需要将加密的文件放在/tmp目录下提供给alice，请写出通过gpg工具实现bob加密文件、alice解密文件的实施步骤，要求采用非对称加密方式。

参考答案

1) alice生成密钥对

```
01. [alice@svr7 ~]$ gpg --gen-key //根据向导完成密钥生成过程
02. [alice@svr7 ~]$ gpg --list-keys //查看公钥信息
```

2) alice将公钥导出

```
01. [alice@svr7 ~]$ gpg --export -a alice > /tmp/alice.key
```

3) bob导入alice的公钥并查看

```
01. [bob@svr7 ~]$ gpg --import /tmp/alice.key
02. [bob@svr7 ~]$ gpg --list-keys
```

4) bob加密文件并将其放入/tmp目录

```
01. [bob@svr7 ~]$ echo "this is a test" > bob.txt
02. [bob@svr7 ~]$ gpg -e alice bob.txt
03. [bob@svr7 ~]$ cp bob.txt.asc /tmp
```

5) alice解密文件

- ```
01. [alice@svr7 ~]$ cp /tmp/jerry.txt.asc .
02. [alice@svr7 ~]$ gpg jerry.txt.asc
```

## 3 AIDE是什么软件？

## 参考答案

AIDE是一套入侵检测系统，该系统通过检查文件或目录的权限、时间、Hash值等检查文件是否被人篡改过。

## 4 下面哪些是aide的配置文件的？

## 参考答案

/etc/aide.conf。

## 5 阅读下列nmap扫描操作，根据注释的功能要求在括号中补全命令选项

- ```
01. [root@svr7 ~]# nmap - ( ) svr7.tarena.com //扫描开启的UDP服务
02. 53/udp open domain
03. [root@svr7 ~]# nmap - ( ) ( ) 192.168.4.0/24 //扫描哪些主机开放FTP、
04. [root@svr7 ~]# nmap - ( ) 192.168.4.110 //扫描操作系统类型
```

参考答案

- ```
01. [root@svr7 ~]# nmap - (sU) svr7.tarena.com //扫描开启的UDP服务
02. 53/udp open domain
03. [root@svr7 ~]# nmap - (p) (21-22) 192.168.4.0/24 //扫描哪些主机开放FT
04. [root@svr7 ~]# nmap - (A) 192.168.4.110 //扫描操作系统类型
```