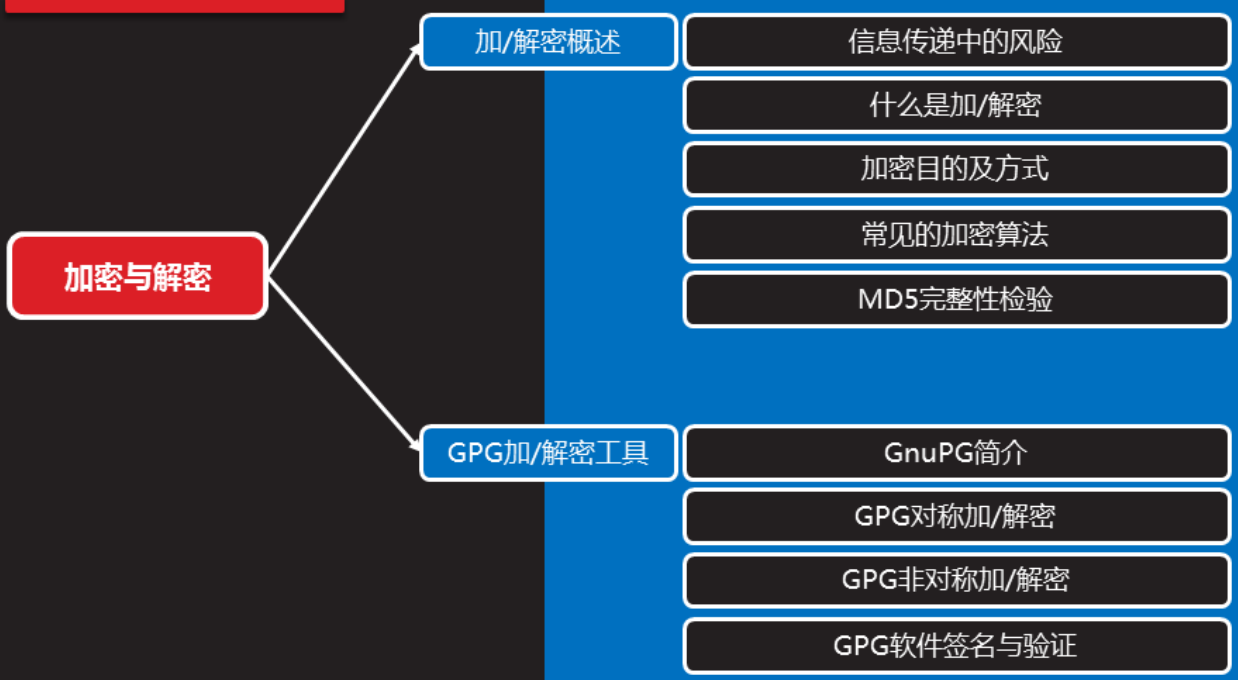
SECURITY DAY02

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	加密与解密
	10:30 ~ 11:20	
	11:30 ~ 12:00	AIDE入侵检测系统
下午	14:00 ~ 14:50	
	15:00 ~ 15:50	扫描与抓包
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑

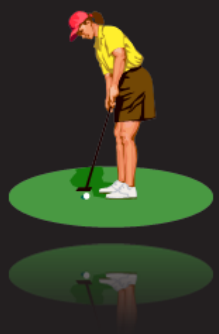
加密与解密



加/解密概述

信息传递中的风险

知识讲解



什么是加/解密

知识讲解

- 发送方：明文 → 密文
  - Tarena ⇨ 加密 ⇨ 25 31 24 23 46 31
- 接收方：密文 → 明文
  - 25 31 24 23 46 31 ⇨ 解密 ⇨ Tarena

加密目的及方式

知识讲解

- 确保数据的机密性
  - 对称加密：加密/解密用同一个密钥
  - 非对称加密：加密/解密用不同的密钥（公钥、私钥）
- 保护信息的完整性
  - 信息摘要：基于输入的信息生成长度较短、位数固定的散列值

常见的加密算法

Tedu.cn 达内教育

知识讲解

- 对称加密
  - DES，Data Encryption Standard
  - AES，Advanced Encryption Standard
- 非对称加密
  - RSA，Rivest Shamirh Adleman
  - DSA，Digital Signature Algorithm

MD5完整性检验

Tedu.cn 达内教育

知识讲解

- 使用md5sum校验工具
  - 生成MD5校验值
  - 与软件官方提供的校验值比对

```
[root@svr7 ~]# md5sum  SuperSOS.iso
fa509cba7c6b5e7ccf430852b59028f5  SuperSOS.iso

[root@svr7 ~]# iptables  -nL | md5sum
31f623f0306de058f2efff372cf5cb44  -
```

GnuPG简介

知识讲解

- GnuPG，GNU Privacy Guard
  - http://www.gnupg.org/
  - 最流行的数据加密、数字签名工具软件

```
[root@svr7 ~]# gpg  --version
gpg (GnuPG) 2.0.14
.. ..
支持的算法：
公钥：RSA, ELG, DSA
对称加密：3DES, CAST5, BLOWFISH, AES, AES256, .. ..
散列：MD5, SHA1, .. .., SHA256, SHA512
```

GPG对称加/解密

知识讲解

- 基本用法
  - 加密操作：--symmetric 或 -c
  - 解密操作：--decrypt 或 -d

```
[root@svr7 ~]# gpg  -c  clear.txt
.. ..                                  //设置密码
[root@svr7 ~]# file clear.txt*
clear.txt:     ASCII text
clear.txt.gpg: data                    //加密后的文件

[root@svr7 ~]# gpg  -d  clear.txt.gpg  > dclear.txt
.. ..                                  //根据提示验证密码
```

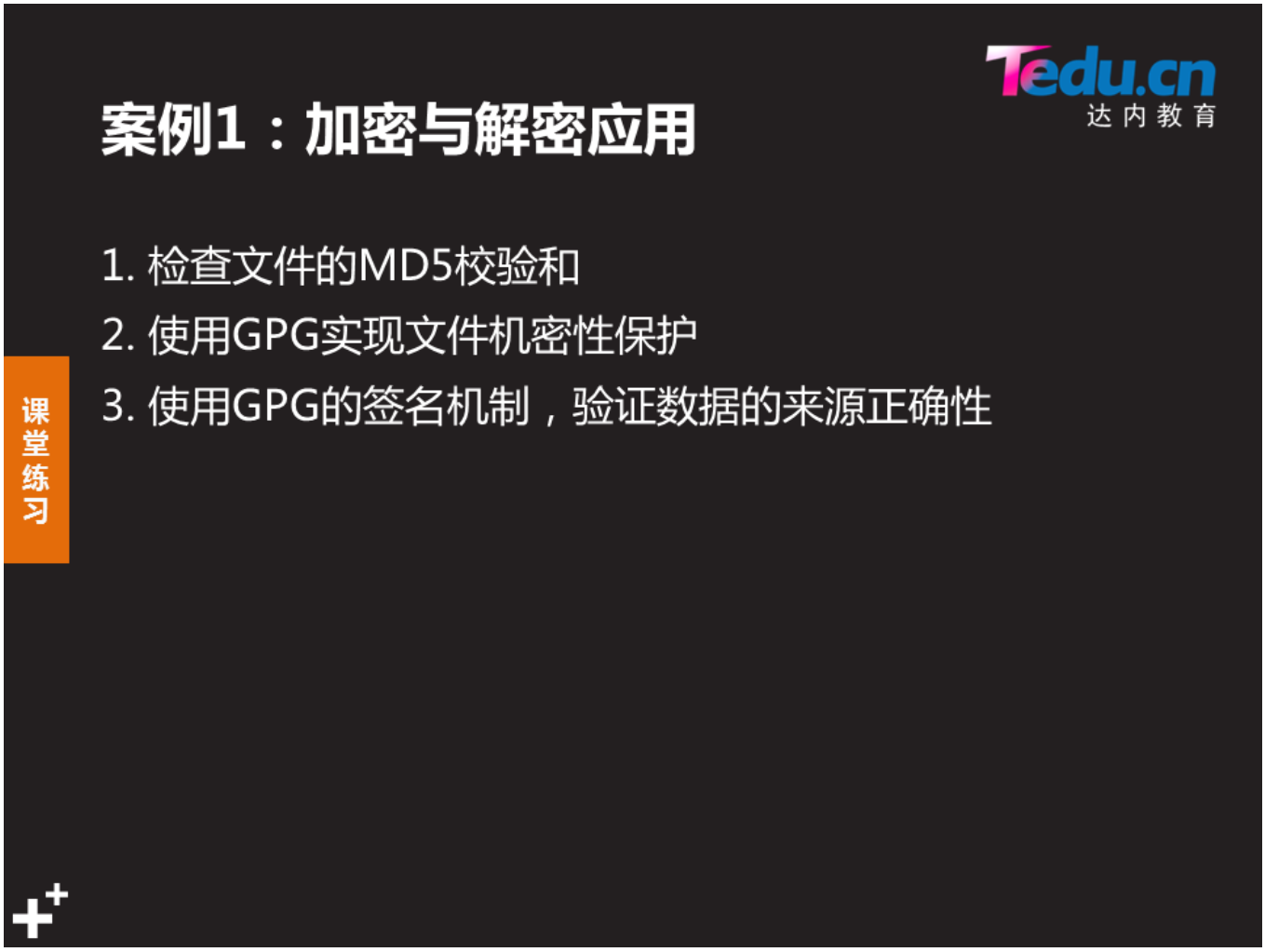
GPG非对称加/解密（续2）

Tedu.cn 达内教育

知识讲解

- 基本用法
  - 加密操作：--encrypt 或 -e
  - 指定目标用户：--recipient 或 -r
  - 解密操作：--decrypt 或 -d

```
[usera@svr7 ~]$ gpg  -e  -r  userb  clear.txt                    //加密
[usera@svr7 ~]$ mv  clear.txt.gpg  /tmp/
.. ..
[userb@svr7 ~]$ gpg  -d  /tmp/clear.txt.gpg  >  dclear.txt  //解密
```


Tedu.cn
达内教育
案例1：加密与解密应用
1. 检查文件的MD5校验和
2. 使用GPG实现文件机密性保护
3. 使用GPG的签名机制，验证数据的来源正确性
课堂练习

安装软件包

Tedu.cn 达内教育

知识讲解

- AIDE(Advanced intrusion detection environment)
- 该软件为一套入侵检测系统
- 配置yum源即可安装aide软件

```
[root@svr7 ~]# yum  -y  install   aide
```

修改配置文件

Tedu.cn 达内教育

知识讲解

- AIDE默认配置文件为/etc/aide.conf

```
[root@svr7 ~]# vim /etc/aide.conf
@@define DBDIR /var/lib/aide                    //数据库目录
@@define LOGDIR /var/log/aide                   //日志目录
database_out=file:@@{DBDIR}/aide.db.new.gz      //数据库文件名
#p:      permissions                            //希望检查的项目
#i:      inode:
#n:      number of links
#u:      user
#g:      group
#s:      size
#md5:    md5 checksum
#sha1:   sha1 checksum
#sha256:       sha256 checksum
FIPSR = p+i+n+u+g+s+m+c+acl+selinux+xattrs+sha256
```

修改配置文件（续1）

Tedu.cn 达内教育

知识讲解

- AIDE默认配置文件为/etc/aide.conf

```
[root@svr7 ~]# vim /etc/aide.conf
/boot   NORMAL                  //对哪些目录进行什么校验
/bin    NORMAL
/sbin   NORMAL
/lib    NORMAL
/lib64  NORMAL
/opt    NORMAL
/usr    NORMAL
/root   NORMAL
!/usr/src                       //使用[!]，设置不校验的目录
!/usr/tmp
```

初始化检查

Tedu.cn 达内教育

知识讲解

- 在没有被攻击入侵前
- 根据配置文件，对数据进行校验操作

```
[root@svr7 ~]# aide --init
AIDE, version 0.15.1
AIDE database at /var/lib/aide/aide.db.new.gz initialized.
```

入侵检查

执行入侵检查

知识讲解

- 将之前备份的校验数据库文件还原

```
[root@svr7 ~]# cp /media/  /var/lib/aide/aide.db.gz
```

- 根据数据库执行入侵检测

```
[root@svr7 ~]# aide --check
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2046-13-45 24:24:24
Summary:
Total number of files: 147173
Added files: 1
Removed files: 0
Changed files: 2
```

为什么需要扫描？

Tedu.cn 达内教育

知识讲解

- 以获取一些公开/非公开信息为目的
  - 检测潜在的风险
  - 查找可攻击目标
  - 收集设备/主机/系统/软件信息
  - 发现可利用的安全漏洞

NMAP应用示例

Tedu.cn 达内教育

知识讲解

- 检查目标主机开放了哪些端口

```
[root@svr7 ~]# nmap  svr7.tedu.cn                    //默认扫描TCP
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
.. ..
[root@svr7 ~]# nmap   -sU  svr7.tedu.cn              //指定-sU扫描UDP
53/udp   open          domain
111/udp  open          rpcbind
631/udp  open|filtered ipp
.. ..
```


Tedu.cn
达内教育
网络抓包工具