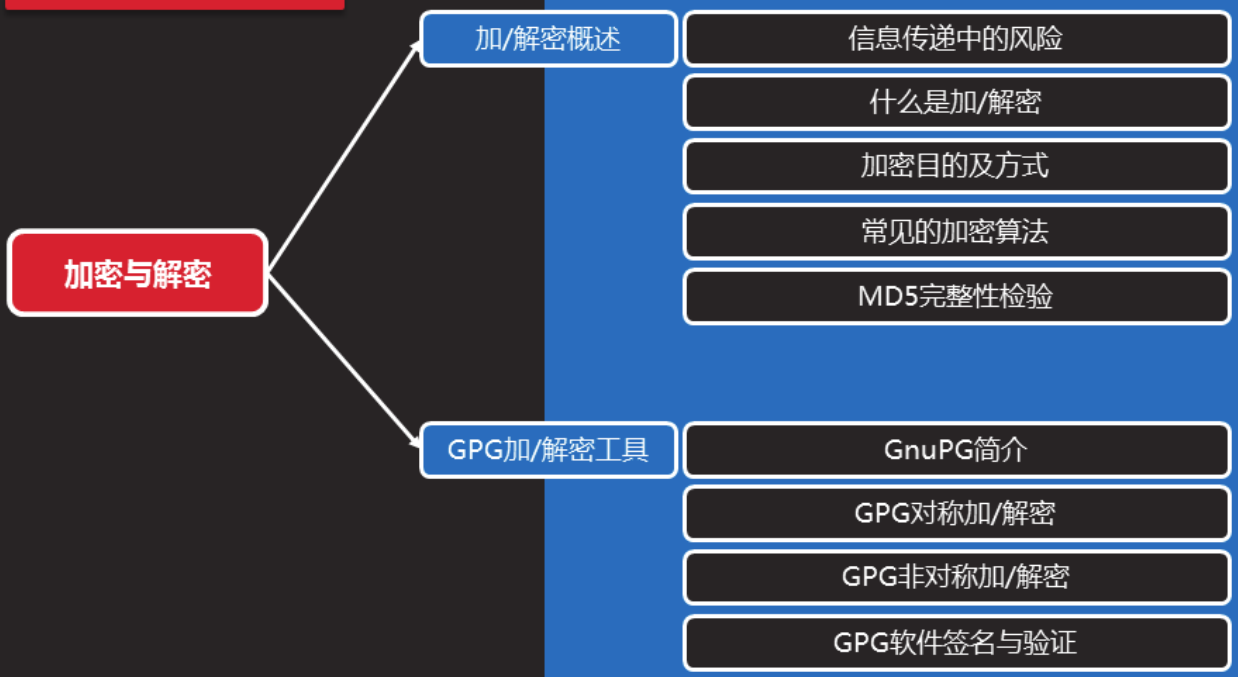
SECURITY DAY02

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

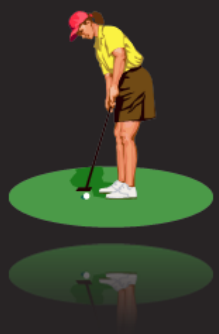
加密与解密



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

常见的加密算法（续1）

Tedu.cn 达内教育

知识讲解

- Hash散列技术，用于信息摘要
  - MD5，Message Digest Algorithm 5
  - SHA，Secure Hash Algorithm

1. 根据输入的文本（长度不限），生成固定长度（比如128位）的摘要文本
2. 只要输入的文本不同，则生成的摘要文本也不一样

MD5完整性检验

- 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

知识讲解

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

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

GPG加/解密工具

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

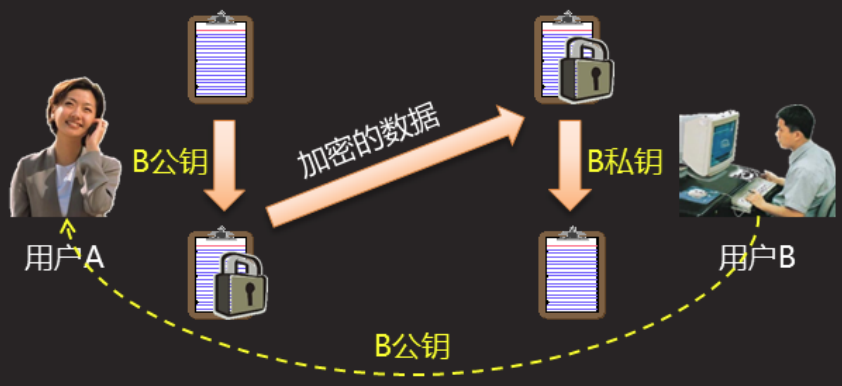
```
[root@svr7 ~]# gpg  -c  clear.txt
.. ..                                  //设置密码
[root@svr7 ~]# file clear.txt*
clear.txt:     ASCII text
clear.txt.gpg: data                    //加密后的文件

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

GPG非对称加/解密

Tedu.cn 达内教育

知识讲解

- 基本过程



01:用户B把自己的公钥传给用户A
02:用户A使用B的公钥加密数据，将加密后的数据给用户B
03:用户B使用自己的私钥解密数据

GPG非对称加/解密（续1）

Tedu.cn 达内教育

知识讲解

- 前期准备工作
  - UserB 创建密钥对：--gen-key
  - UserB 导出公钥：--export、--armor 或 -a
  - UserA 导入公钥：--import

```
[userb@svr7 ~]$ gpg  --gen-key
.. ..   // 设置用户信息、私钥口令
[userb@svr7 ~]$ gpg  --list-keys
[userb@svr7 ~]$ gpg  -a  --export  userb  >  /tmp/UserB.pub
.. ..
[usera@svr7 ~]$ gpg  --import  /tmp/UserB.pub
```

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
```

GPG软件签名与验证

Tedu.cn 达内教育

知识讲解

- 软件签名与验证过程
  - 软件官方以私钥对软件包执行数字签名
  - 用户下载软件包、软件官方的公钥
  - 以官方公钥验证软件包签名，确保数据来源正确

GPG软件签名与验证（续1）

知识讲解

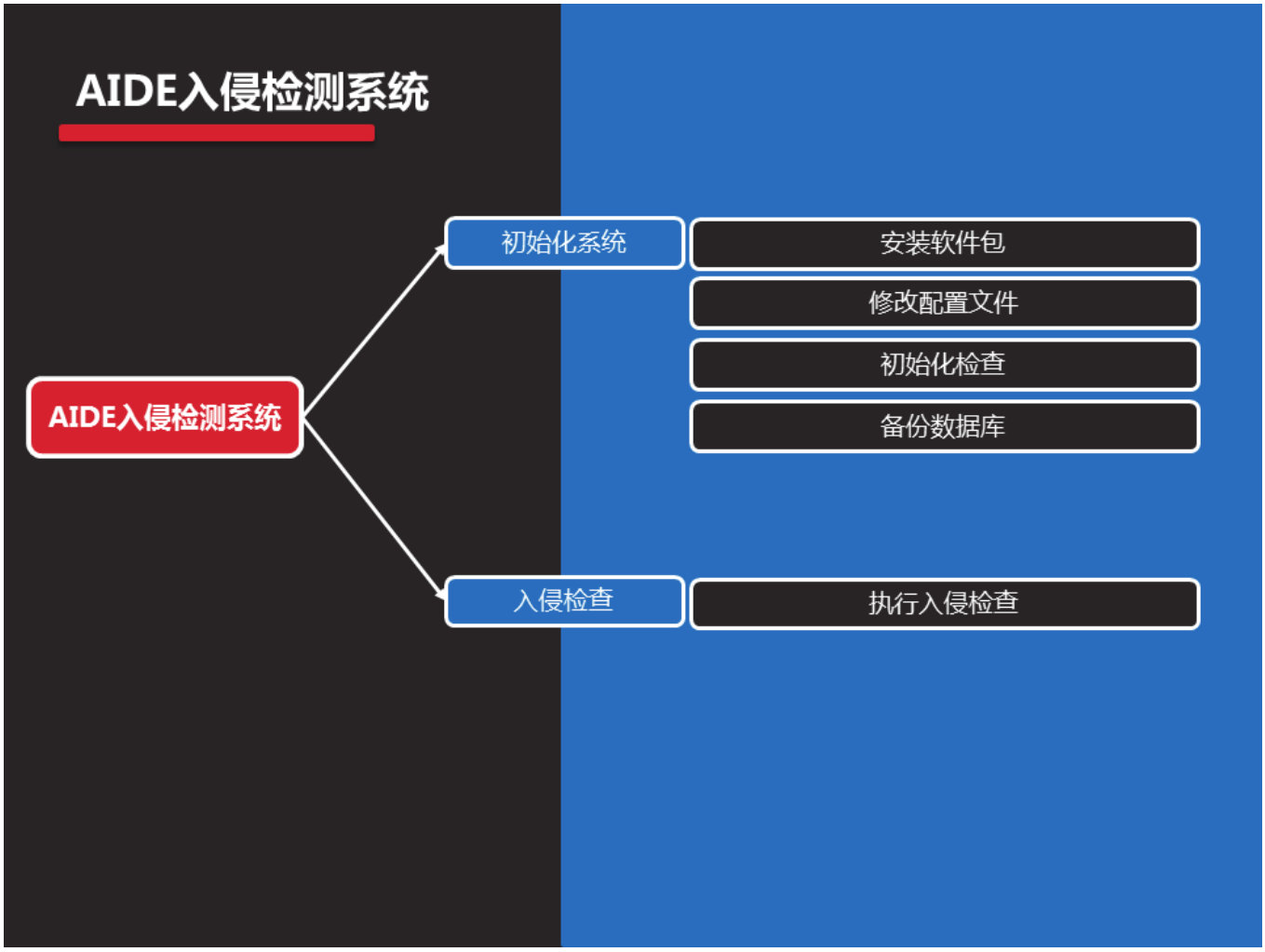
- 为软件包建立签名文件
  - 分离式签名：--detach-sign 或 -b
- 验证软件包签名
  - 验证签名：--verify

```
[userb@svr7 ~]$ gpg  -b  /tmp/DenyHosts-2.6.tar.gz
.. ..

[usera@svr7 ~]$ gpg  --import  /tmp/UserB.pub  //导入官方公钥
[usera@svr7 ~]$ gpg  --verify  /tmp/DenyHosts-2.6.tar.gz.s\
>ig  /tmp/DenyHosts-2.6.tar.gz
.. .. gpg: 完好的签名，来自于“userb (User B) <userb@tedu.cn>”
```

案例1：加密与解密应用

课堂练习

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


AIDE入侵检测系统
AIDE入侵检测系统
初始化系统
安装软件包
修改配置文件
初始化检查
备份数据库
入侵检查
执行入侵检查


Tedu.cn
达内教育
初始化系统

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）

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

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.
```

备份数据库

- 在被入侵前，将校验的数据库文件备份到安全的地方
- 如，优盘、光盘、移动硬盘、网络存储

知识讲解

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

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
```

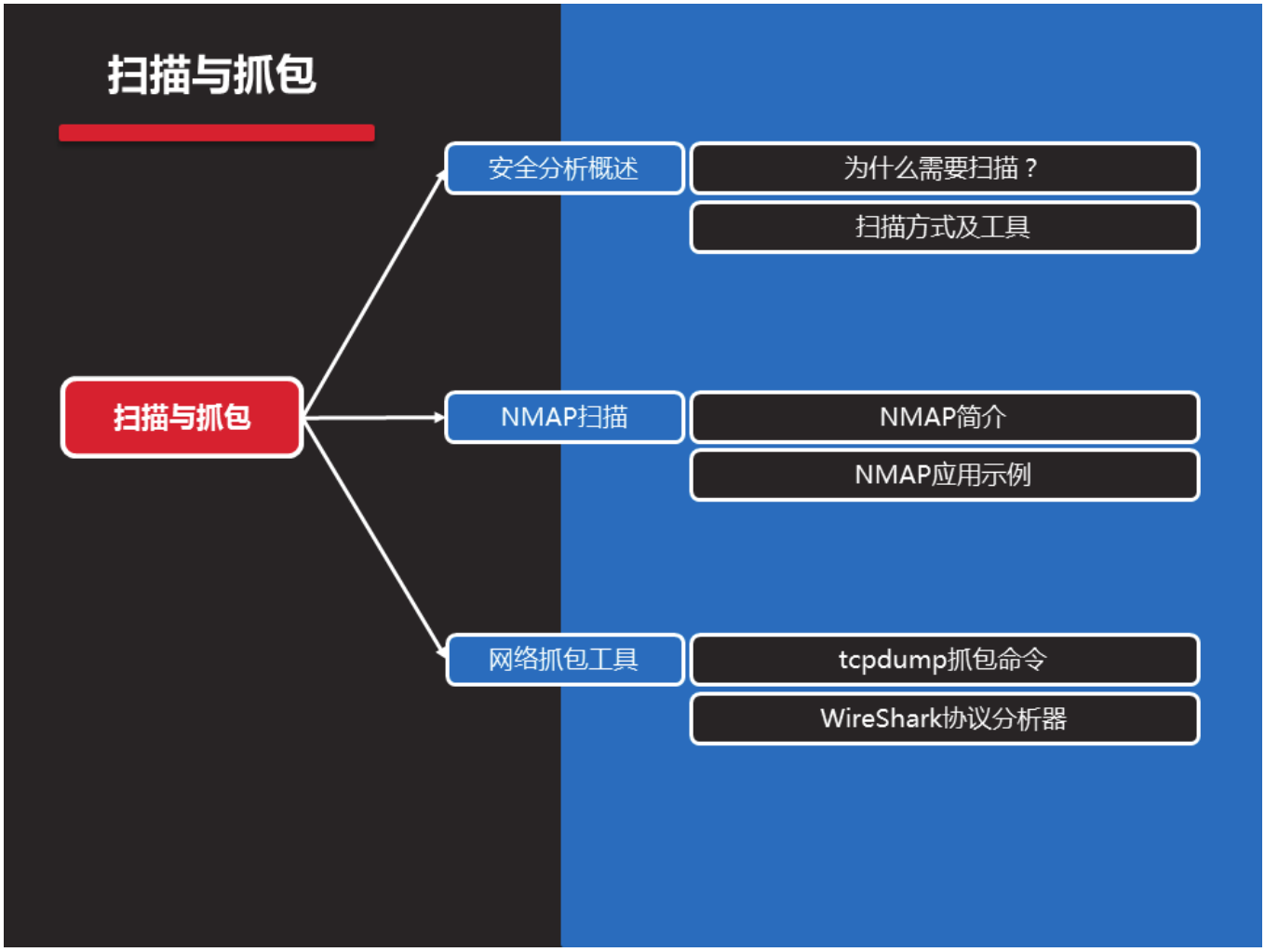
- 根据数据库执行入侵检测

```
[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
```

案例2：使用AIDE做入侵检测

课堂练习

1. 安装aide软件
2. 执行初始化校验操作，生成校验数据库文件
3. 备份数据库文件到安全的地方
4. 使用数据库执行入侵检测操作


扫描与抓包
扫描与抓包
安全分析概述
为什么需要扫描？
扫描方式及工具
NMAP扫描
NMAP简介
NMAP应用示例
网络抓包工具
tcpdump抓包命令
WireShark协议分析器


Tedu.cn
达内教育
安全分析概述

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

扫描方式及工具

Tedu.cn 达内教育

知识讲解

- 典型的扫描方式
  - Scan，主动探测
  - Sniff，被动监听/嗅探
  - Capture，数据包捕获（抓包）

扫描方式及工具（续1）

Tedu.cn 达内教育

- 常见的安全分析工具
  - 扫描器：NMAP
  - 协议分析：tcpdump、WireShark

知识讲解

Tedu.cn 达内教育

NMAP扫描

NMAP简介

知识讲解

- 一款强大的网络探测利器工具
- 支持多种探测技术
  - ping 扫描
  - 多端口扫描、
  - TCP/IP指纹校验
  - ……

NMAP简介（续1）

知识讲解

- 基本用法
  - nmap [扫描类型] [选项] <扫描目标 ...>
- 常用的扫描类型
  - -sS，TCP SYN扫描（半开）
  - -sT，TCP 连接扫描（全开）
  - -sU，UDP扫描
  - -sP，ICMP扫描
  - -A，目标系统全面分析

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
.. ..
```

NMAP应用示例（续1）

Tedu.cn 达内教育

知识讲解

- 检查哪些主机开启FTP、SSH服务端

```
[root@svr7 ~]# nmap  -p  21-22  192.168.4.0/24
Nmap scan report for 192.168.4.100
21/tcp closed ftp
22/tcp open   ssh
.. ..
Nmap scan report for 192.168.4.110
21/tcp open    ftp
22/tcp closed ssh
.. ..
```

NMAP应用示例（续2）

Tedu.cn 达内教育

知识讲解

- 检查目标主机的存活状态（是否可ping通）

```
[root@svr7 ~]# nmap  -n  -sP  192.168.4.0/24
Nmap scan report for 192.168.4.100
Host is up (0.00027s latency).
.. ..
Nmap scan report for 192.168.4.110
Host is up (0.00018s latency).
.. ..
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.26
seconds.. ..
```

NMAP应用示例（续3）

Tedu.cn 达内教育

知识讲解

- 检查操作系统指纹

```
[root@svr7 ~]# nmap  -A  192.168.4.110
.. ..
.. ..

Host script results:
|_nbstat: NetBIOS name: ZY-T430, NetBIOS user: <unknown>,
NetBIOS MAC: 00:50:56:c0:00:01 (VMware)
|_smbv2-enabled: Server supports SMBv2 protocol
| smb-os-discovery:
|   OS: Windows 8 Enterprise 9200 (Windows 8 Enterprise 6.2)
|   Name: WORKGROUP\ZY-T430
|_  System time: 2013-08-08 17:06:32 UTC+8
.. ..
```

-A 是一个复合选项，相当于：
-O（OS检测）、-sV（版本检测）、-sC（脚本检测）、traceroute跟踪、...

网络抓包工具

tcpdump抓包命令

知识讲解

- 一款提取TCP数据包的命令行工具
- 基本用法
  - tcpdump [选项] [过滤条件]
- 常见监控选项
  - -i， 指定监控的网络接口
  - -A，转换为 ACSII 码，以方便阅读
  - -w，将数据包信息保存到指定文件
  - -r， 从指定文件读取数据包信息

tcpdump抓包命令（续1）

Tedu.cn 达内教育

知识讲解

- tcpdump的过滤条件
  - 类型：host、net、port、portrange
  - 方向：src、dst
  - 协议：tcp、udp、ip、wlan、arp、……
  - 多个条件组合：and、or、not

tcpdump抓包命令（续2）

Tedu.cn 达内教育

知识讲解

- 应用示例：
  - 按条件（访问指定的POP3服务）抓取数据包
  - 按 Ctrl+c 键停止抓包

```
[root@svr7 ~]# \
 tcpdump -A dst host 192.168.4.5 and tcp port 110
.. ..
10:00:32.249208 IP 192.168.4.5.33627 > 192.168.4.100.pop3:
...O.... user mickey
.. ..
10:00:34.968173 IP 192.168.4.5.33627 > 192.168.4.100.pop3:
........ pass 123456
.. ..
```

tcpdump抓包命令（续3）

知识讲解

- 保存、分析抓包结果
  - 抓取访问FTP服务的包，保存为cap文件

```
[root@svr7 ~]# tcpdump  -A  -w  ftp.cap  \          //抓包并保存
> host 192.168.4.5  and  tcp  port  21
.. ..
^C .. ..

[root@svr7 ~]#   tcpdump  -A  -r  ftp.cap | egrep  '(USER|PASS)'
                                                    //分析抓取结果
reading from file ftp0809.cap, link-type EN10MB (Ethernet)
E..2.~@.@..y...x.....&...}.a...+P.....USER ftp
E..5..@.@..t...x.....&...}.k...MP.....PASS 123456
.. ..
```

WireShark协议分析器

知识讲解

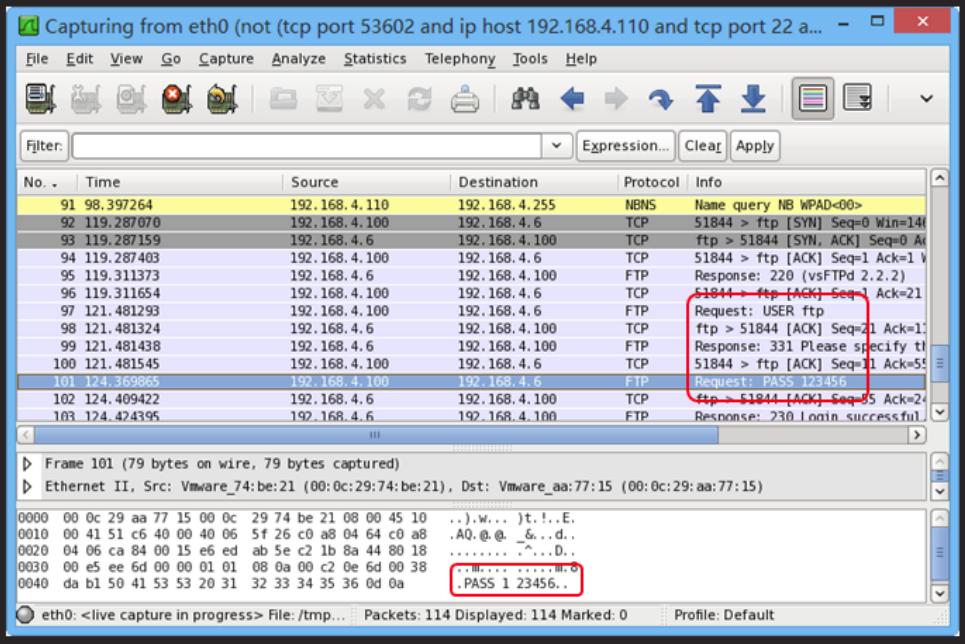
- 一款与tcpdump类似的抓包工具，需要图形环境
  - http://www.wireshark.org/
- RHEL光盘中的2个包
  - wireshark
  - wireshark-gnome

WireShark协议分析器（续1）

Tedu.cn 达内教育

知识讲解

了解知识：wireshark抓包的效果如下图，与tcpdump类似，但需要图形



案例3：扫描与抓包分析

Tedu.cn 达内教育

课堂练习

1. 使用NMAP扫描主机/网段
2. 使用tcpdump分析FTP通信过程

总结和答疑

总结和答疑 → 非对称加密原理 → GPG非对称加/解密

Tedu.cn 达内教育

非对称加密原理

GPG非对称加/解密

Tedu.cn 达内教育

- 基本过程

知识讲解