国家计算机软考职称
中级网络工程师培训

第15课：网络安全与应用（二）

微信/QQ383419460，每周一三五 20:30-22:00， 全程录像网盘下载

上节课考点回顾

- 1、网络安全基础
- 2、信息加密技术
- 3、数字签名技术
- 4、密钥管理技术
- 5、虚拟专用网VPN

第15课：网络安全与应用（二）

- ***1、应用层安全协议***
- 2、病毒与木马
- 3、防火墙技术
- 4、IDS和IPS
- 5、网工考题分析

【章节】网工：8.9-8.12

第15课：网络安全与应用（二）

- **考点01：**应用层安全协议SHTTP和HTTPS：

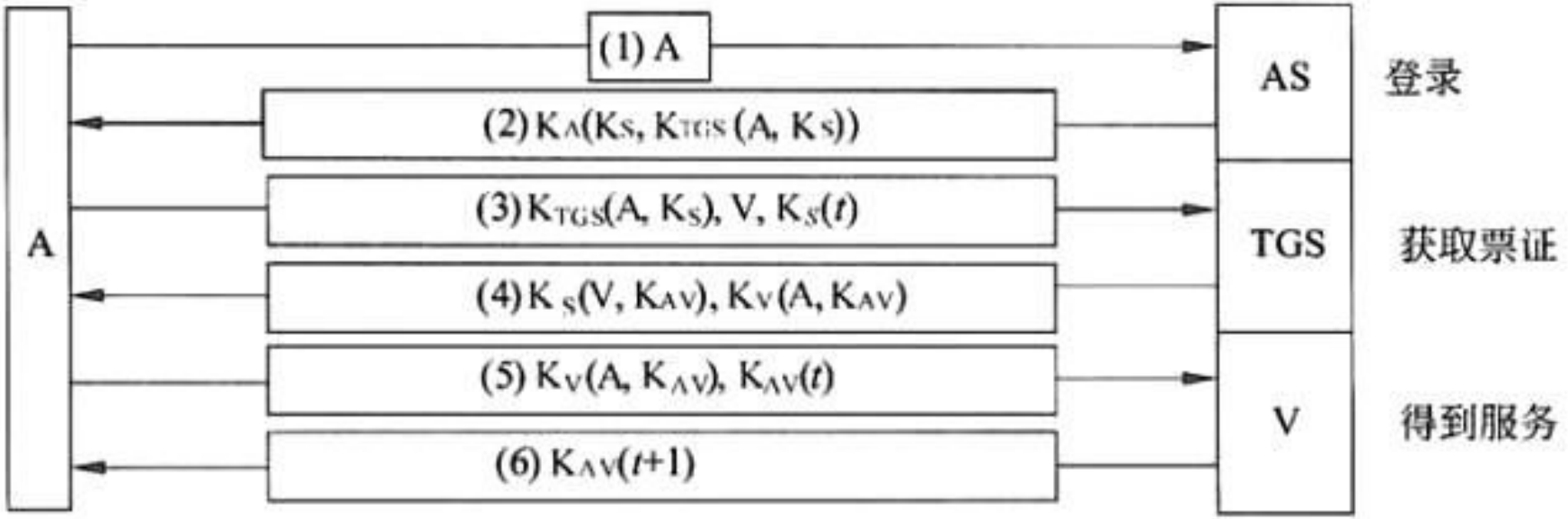
- SHTTP：Sec HTTP，安全超文本传输协议，是HTTP扩展，使用TCP的80端口。

- HTTPS：HTTP+SSL，使用TCP的443端口。大部分web应用采用这个。

- SET：安全的电子交易，主要应用电子商务。

第15课：网络安全与应用（二）

- **考点02：**应用层安全协议Kerberos(刻薄肉丝)：是一项认证服务，3A(AAA)认证有验证、授权和记账。防重放、保护数据完整性。AS认证服务器，TGS票据授予服务器，V应用服务器。



V4时间戳，V5序列号。口诀：无T加T，有T加1。

第15课：网络安全与应用（二）

- 1、应用层安全协议
- ***2、病毒与木马***
- 3、防火墙技术
- 4、IDS和IPS
- 5、网工考题分析

【章节】网工：8.9-8.12

第15课：网络安全与应用（二）

- **考点03：**病毒：一段可执行的程序代码，通过其他可执行程序启动和感染传播，可自我复制，难以清除，破坏性强。（强盗）
- 木马：一种潜伏在计算机里并且秘密开放一个甚至多个数据传输通道的远程控制程序。C/S结构，客户端也称为控制端。偷偷盗取账号、密码等信息。（间谍）
- 恶意代码：又称恶意软件。也称为广告软件、间谍软件，没有作用却会带来危险。（恶搞）

第15课：网络安全与应用（二）

- **考点04：**常见病毒木马的特征分类：
- ①文件宏病毒：感染office文件，前缀Macro或者word/excel等。
- ②蠕虫病毒：前缀Worm通过系统漏洞传播。
- ③木马病毒：前缀Trojan，黑客病毒前缀Hack，往往成对出现。
- ④系统病毒：前缀Win32、PE、Win95等。
- ⑤脚本病毒：前缀Script，脚本语言编写的，通过网页传播。

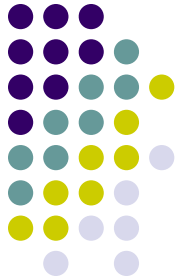
第15课：网络安全与应用（二）

- **考点05：**黑客与骇客：黑客技术高超，帮助测试建设网络。骇客专门搞破坏或恶作剧。

- 黑客攻击：①拒绝服务攻击。②缓冲区溢出攻击。③漏洞攻击。④欺骗攻击。

- 攻击预防：安装杀毒软件和防火墙，合理设置安全策略。

第15课：网络安全与应用（二）

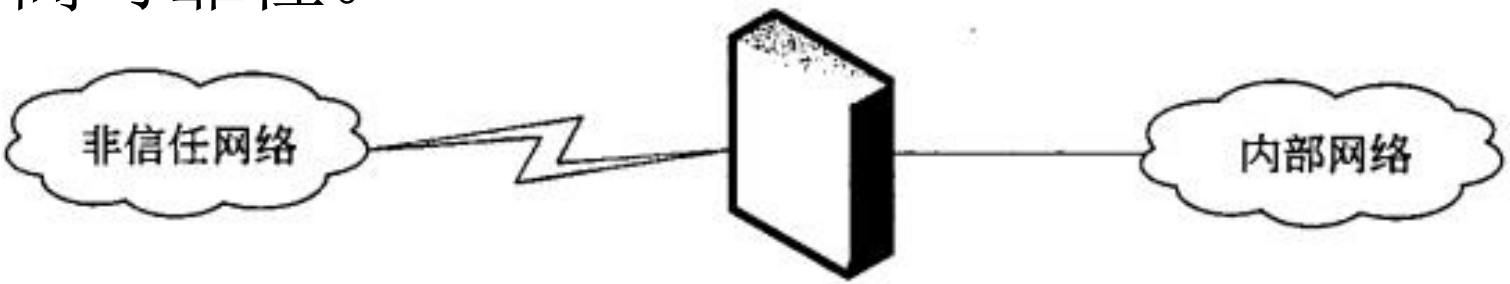


- 1、应用层安全协议
- 2、病毒与木马
- ***3、防火墙技术***
- 4、IDS和IPS
- 5、网工考题分析

【章节】网工：8.9-8.12

第15课：网络安全与应用（二）

- **考点10：**防火墙的定义：来源于建筑物“防火墙”一词，位于两个或多个网络之间，执行访问控制策略，过滤进出数据包的一种软件或硬件设备。
- 防火墙的要求：①所有进出网络的通信流量都必须经过防火墙。②只有内部访问策略授权的通信才能允许通过。③防火墙本身具有很强的高可靠性。



第15课：网络安全与应用（二）

- **考点11：**防火墙的主要功能：①访问控制功能。②内容控制功能。③全面的日志功能。④集中管理功能。⑤自身的安全功能。

- 防火墙的附加功能：①流量控制。②网络地址转换NAT。③虚拟专用网VPN。

- 防火墙的局限性：①关闭限制了一些服务带来不便。②对内部的攻击无能为力。③带来传输延迟单点失效等。④还有其他局限。

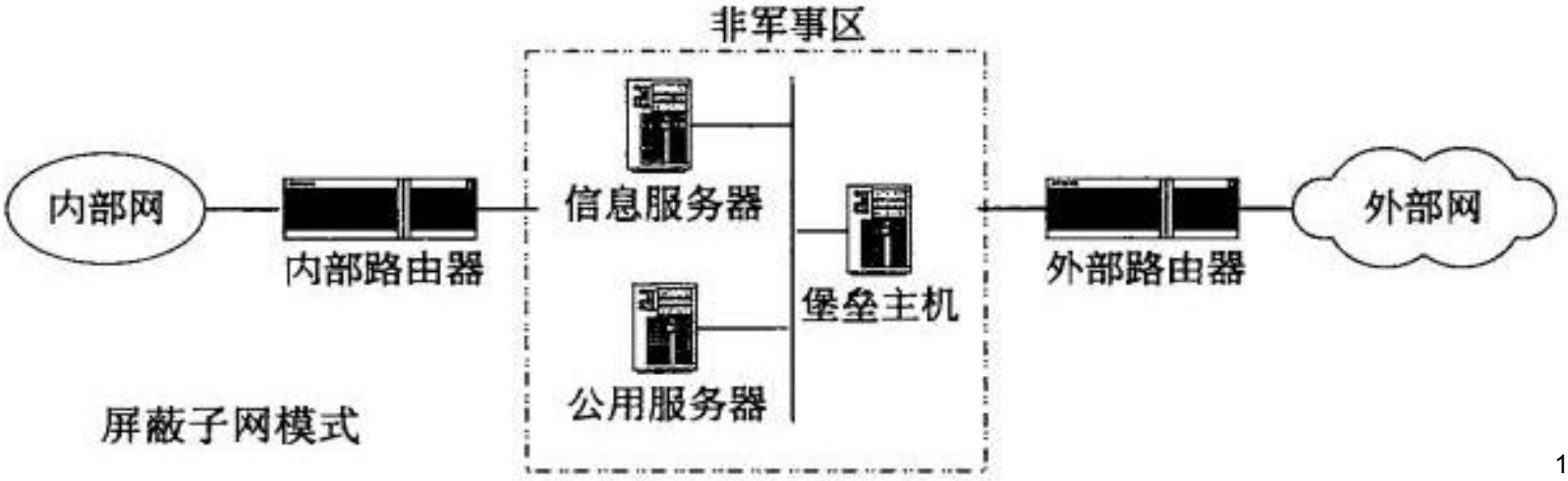
第15课：网络安全与应用（二）

- **考点12：**防火墙的体系结构：①双宿主机模式：防火墙具有两个网卡接口，通过包过滤代理访问网络。这是比较简单的一种结构。一般可以根据IP地址和端口号进行过滤。

双宿主机模式

第15课：网络安全与应用（二）

- **考点12：**防火墙的体系结构：②屏蔽子网模式：又叫过滤子网模式，两个包过滤路由器中间建立一个隔离的子网，定义为DMZ网络，也称为非军事化区域。这是目前防火墙最常用的一种模式。可以有更高级的功能。



屏蔽子网模式

第15课：网络安全与应用（二）

- **考点13：**防火墙PIX的配置简介：Cisco的硬件防火墙，典型的设备是PIX525。

- 三种接口：①内部接口（inside）：连接内网和内网服务器。②外部接口（outside）：连接外部公共网络。③中间接口（DMZ）：连接对外开放服务器。

- 常用命令有：nameif、interface、ip address、nat、global、route、static、conduit、fixup、telnet等。

第15课：网络安全与应用（二）

- **考点14：**防火墙nameif、interface、ip add

```
PIX525#conf t                                                    //进入配置模式
PIX525(config)#nameif ethernet0 outside security 0               //设置安全级 0
PIX525(config)#nameif ethernet1 inside security100               //设置安全级 100
PIX525(config)#nameif ethernet2 dmz security 50                  //设置安全级 50

PIX525(config)#interface ethernet0 auto                          //设置自动方式
PIX525(config)#interface ethernet1 100full                       //设置全双工方式
PIX525(config)#interface ethernet2 100full                       //设置全双工方式

PIX525(config)#ip address outside 133.0.0.1 255.255.255.252      //设置接口 IP
PIX525(config)#ip address inside 10.66.1.200 255.255.0.0         //设置接口 IP
PIX525(config)#ip address dmz 10.65.1.200 255.255.0.0            //设置接口 IP
```

第15课：网络安全与应用（二）

- **考点15：**防火墙global、nat、route、acl

```
PIX525(config)#global (outside) 1 133.1.0.1-133.1.0.14          //定义的地址池
PIX525(config)#nat (inside) 1 0 0                                //0 0 表示所有

PIX525(config)#route outside 0 0 133.0.0.2                       //设置默认路由

PIX525(config)#static (dmz，outside) 133.1.0.1 10.65.1.101       //静态 NAT
PIX525(config)#static (dmz，outside) 133.1.0.2 10.65.1.102       //静态 NAT
PIX525(config)#static (inside，dmz) 10.65.1.200 10.66.1.200      //静态 NAT

PIX525(config)#access-list 101 permit ip any host 133.1.0.1 eq www   //设置 ACL
```

第15课：网络安全与应用（二）

- **考点16：**防火墙访问规则：

1、inside可以访问任何outside和dmz区域

2、dmz可以访问outside区域

3、outside访问dmz需配合static(静态地址转换)

4、inside访问dmz需要配合acl(访问控制列表)

- 其他软件防火墙：天网防火墙、ISA Server（微软公司）。

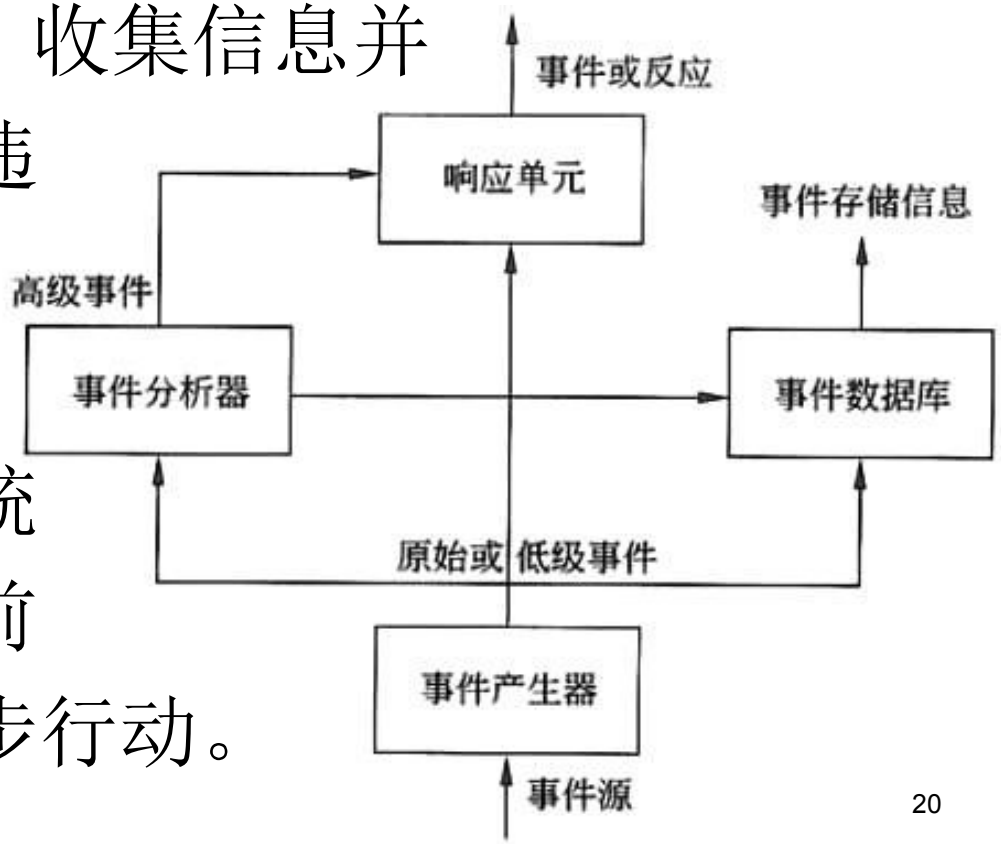
第15课：网络安全与应用（二）

- 1、应用层安全协议
- 2、病毒与木马
- 3、防火墙技术
- ***4、IDS和IPS***
- 5、网工考题分析

【章节】网工：8.9-8.12

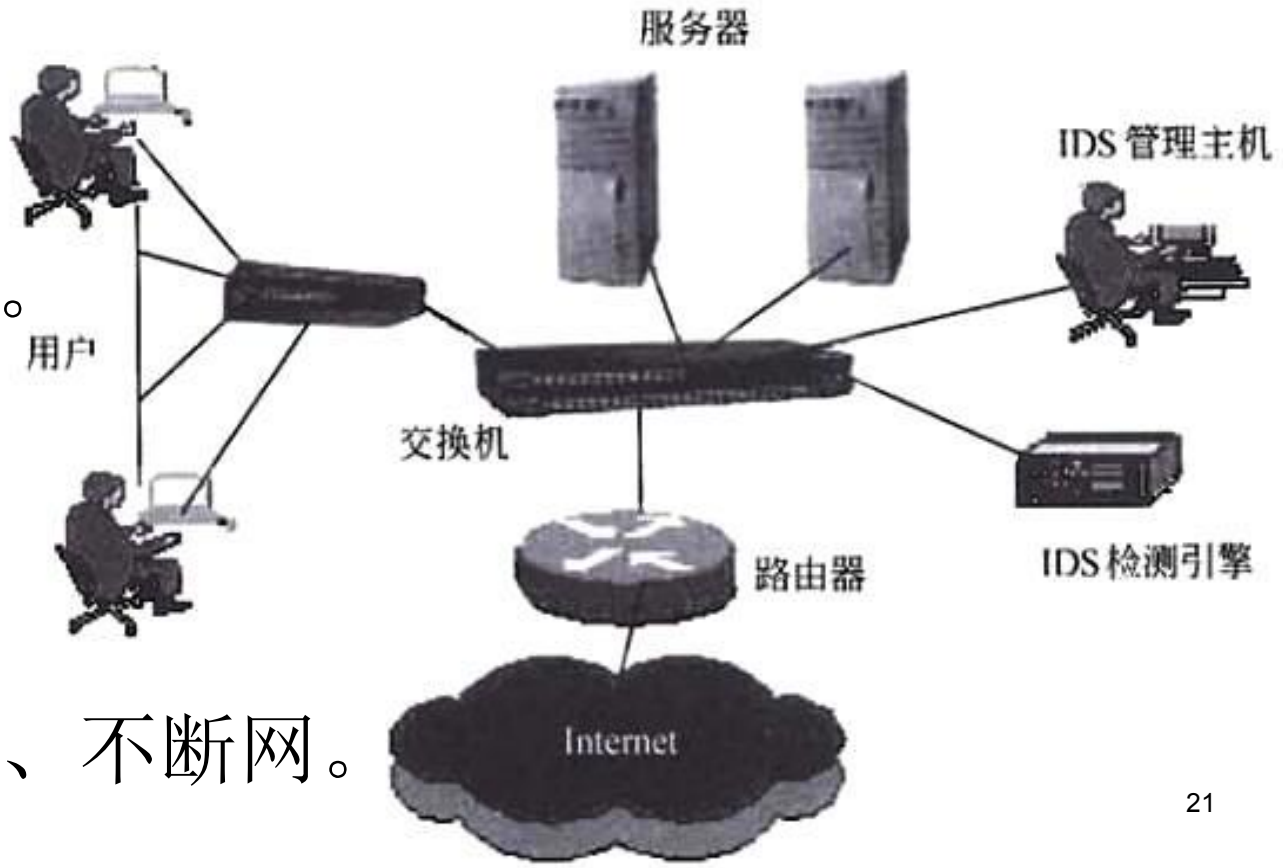
第15课：网络安全与应用（二）

- **考点17：**入侵检测系统IDS：位于防火墙之后的第二道安全屏障，是防火墙的的有力补充。通过对网络关键点 收集信息并对其分析，检测到违反安全策略的行为和入侵的迹象，做出自动反应，在系统损坏或数据丢失之前阻止入侵者的进一步行动。



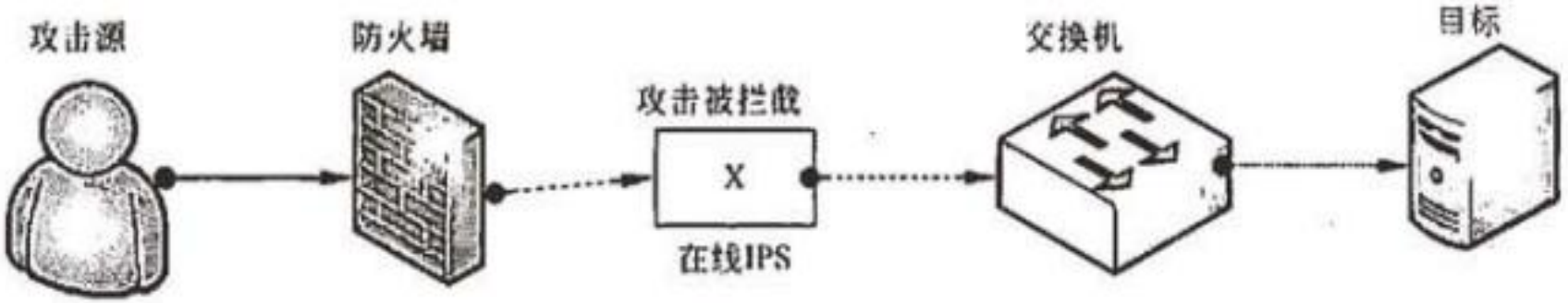
第15课：网络安全与应用（二）

- **考点18：**入侵检测系统IDS：安装部署位置通常是：①服务器区域的交换机上。②Interner接入路由器之后的第一台交换机上。③其他重点保护网段的交换机上。
- 通常是并联、不断网。



第15课：网络安全与应用（二）

- **考点18：**入侵防御系统IPS：位于防火墙之后的第二道安全屏障，是防火墙的的有力补充。通过对网络关键点　收集信息并对其分析，检测到攻击企图，就会自动将攻击包丢掉或采取措施阻挡攻击源，切断网络。



- 通常是串联、会断网。

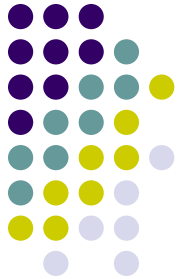
第15课：网络安全与应用（二）

- **考点19：**IPS/IDS和防火墙区别：防火墙一般只检测网络层和传输层的数据包，不能检测应用层的内容。IPS/IDS可以检测字节内容。

- IPS和IDS的区别：IPS是串接在网络中，会切断网络。IDS是旁路式并联在网络上，不切断网络。

- IDS/IPS：连接在需要把交换机端口配置成镜像端口上，可以检测到全网流量。

第15课：网络安全与应用（二）



- 1、应用层安全协议
- 2、病毒与木马
- 3、防火墙技术
- 4、IDS和IPS
- ***5、网工考题分析***

【章节】网工：8.9-8.12

例题01

- 下列网络攻击行为中，属于DDOS攻击的是（　　）。

A. 特洛伊木马攻击　　B. SYN Flooding攻击

C. 端口欺骗攻击　　D. IP欺骗攻击

例题02

- HTTPS的安全机制工作在（　　）。

A. 网络层　　B. 传输层　　C. 应用层　　D. 物理层

例题03

- 包过滤防火墙对通过防火墙的数据包进行检查，只有满足条件的数据包才能通过，对数据包的检查内容一般不包括（　　）。

A. 源地址　　B. 目的地址

C. 协议　　D. 有效载荷

例题04

在X.509标准中，不包含在数字证书中的数据域是（　　）。 A. 序列号　　B. 签名算法

C. 认证机构的签名　　D. 私钥

例题05

- 关于入侵检测系统的描述，错误的是（　　）。

  A. 监视分析用户及系统活动

  B. 发现并阻止一些未知的攻击活动

  C. 检测违反安全策略的行为

  D. 识别已知进攻模式并报警

例题06

- 主动攻击不包括（　　）。

  A. 假冒　B. 重放　C. 修改消息　D. 泄露信息

例题答案

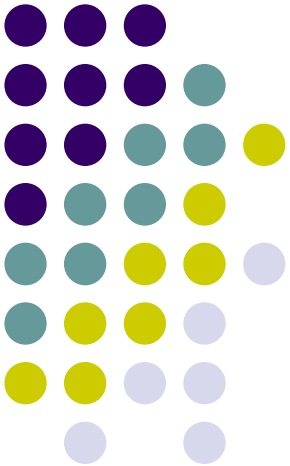
- 例题01：B。
- 例题02：B。
- 例题03：D。
- 例题04：D。
- 例题05：B。
- 例题06：D。

- **作业：01号题库17、18**

获取考试咨询帮助加老师
微信/QQ 383419460

大涛网络学院 出品

UU教育 2017.8月



微信/QQ383419460，每周一三五 20:30-22:00， 全程录像网盘下载